System Administration

Arizona AIM System
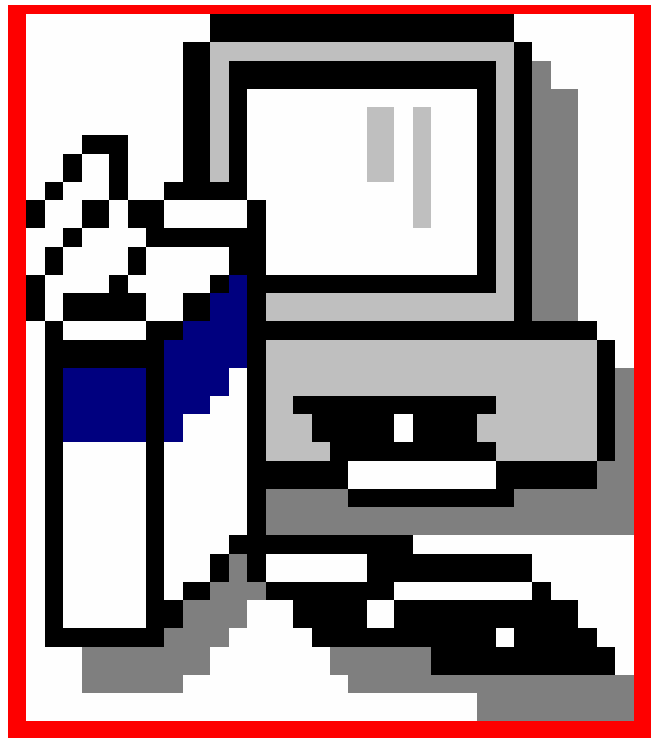
Table of Contents

Chapter 7 - Systems Administration

Capabilities

Purpose

The System Administration functional area is intended to contribute to the overall flexibility, efficiency, and security required for operating and maintaining the AIM System. The functions included in this area are not necessarily WIC Program requirements; they are standard features of a well-designed automated system. This functional area provides the capabilities to maintain information contained in system data (reference) tables, to control general access to the system as well as the ability to perform specific functions, and to move certain files to off-line storage for increased system efficiency.

Table Maintenance

Maintain System Data Tables

State and Local agencies must have the flexibility to adapt to periodic changes in food packages, clinic sites, nutrition measurement, vendor risk and other elements of the WIC Program. In an automated WIC System, many of these data elements are stored in data tables used for data validation and other internal system processes. For efficiency, most of these data elements are stored as one or two-digit codes. Each code typically has a full text translation. These codes and accompanying text are established by the State Agency. Data elements contained in data tables are also shared with one or more data stores.

This information becomes useful for editing data entered into the WIC System. For example, when a participant's information is recorded during enrollment processing, the city entered into the system is compared to the legitimate codes contained in the locales data table. If the code is located in the table, the information is accepted and stored by the system. If, however, the code does not exist in the table, the system returns an error message to the user. Also, all other information associated with the city such as county, state and zip code automatically becomes part of the record.

The ability to maintain the system's data tables is critical to allow the AIM System to easily adapt to changes in the WIC Program. The information in these tables must be current and accurate to ensure the accuracy of the data validation processes that take place in the system. Incomplete or erroneous data in the tables may permit the entry of invalid data, or prevent the entry of legitimate information.

Maintain Cities

The AIM System supports this function by allowing users to capture new and existing cities being used throughout the WIC Program. The records in this table can be selected for use in the

Maintain Locales tables in which users create entire locales made up of city, zip code, county and state.

Maintain Contact Method

The AIM System enables users to maintain contact method data utilized primarily in the Nutrition Education and Vendor Management areas of the system. Consistent, accurate information on the methods utilized in communicating (in-store visit, fax, letter, phone call, etc.) with vendors and/or participants is important in evaluating the program's success.

Maintain Contact Titles

This table serves to capture and maintain cross-reference information about different contact titles used in vendor monitoring. Examples of contact titles include owner, manager, cashier, etc.

Maintain Locales

The System supports the maintenance of all location data utilized within WIC function. A central function enables users to maintain the relationships between cities, counties, and zip codes. These relationships are used throughout the system whenever an address (mailing or street) is captured. This occurs primarily during the maintenance of vendor data or the certification process.

Maintain Phone Types

The WIC application supports the maintenance of phone information. Consistent and accurate phone information is essential since most communications with participants and vendors utilize telecommunications technology.

Maintain States and Counties

The AIM System supports this function by allowing the user to build the relationships between the Counties within the particular State. These relationships are used throughout the system whenever an address is captured. This occurs primarily during the maintenance of vendor data or during the certification process.

Maintain Zip Codes

The System supports the maintenance of 5-digit zip code information utilized by the WIC function. A central function enables users to build and maintain zip codes that are used throughout the application. Zip code 4-digit extensions are maintained in the individual tables that utilize them.

Security

Administer System Security

Federal regulations require that access to WIC information be restricted to authorized individuals. Access to sensitive health and income information must be limited to those individuals at State and Local Agencies who require such information to serve WIC participants. The issuance of food instruments is another sensitive area that requires tighter controls than most other

management information or participant processing functions. The various controls placed on access to the system as a whole as well as these specific areas constitute a large part of system security.

Administering system security is important because it protects the access to information in the AIM System. System security prevents unauthorized individuals from entering or updating WIC information. It also provides a means of ensuring that only those individuals that have been adequately trained in system operations can access any of the system's functions. Finally, accurate identification of the users enables the system to create a complete audit trail of all transactions in the system.

In general, the AIM System supports standard security features such as passwords, timed logouts, and terminal lockup after a given number of unsuccessful system access attempts. The System can distinguish between those capabilities that can be performed by a State Agency user and those that can be performed by a Local Agency user. For example, enrollment processing is usually performed at the local level, while vendor management is primarily the domain of the State Agency. In this specific function, the AIM System allows authorized users at the State Agency level to add, delete, or update user access and identification information in the system.

The System provides the ability to record and control the specific capabilities of each user at a level defined by the State Agency. State and Local agencies also have the capability to record and review attempts at unauthorized access to the AIM System.

Maintain User Identification and Capabilities

The AIM System allows authorized users (usually the system administrator) at the State Agency level to add, delete, or update users in the system. When a new user is entered, the system assigns (or accepts from entry) a User Identification that uniquely identifies the user, associates the user with a specific State or Local Agency, and assigns the user an initial password. All users accessing the WIC application are required to enter their unique ID.

The AIM System controls access to specific functions within the system. Access to these functions is controlled by a series of roles for each User ID in the System that specifies which functions the user is authorized to perform. For example, a clerk may be allowed to enter enrollment data, but not allowed to issue a food instrument. The System allows the State-level system administrator to create and modify the roles that are used.

The System enables authorized users (e.g., the AIM System Administrator) at the agency level to update these role assignments for each user at their specific site. The System provides a display window that identifies the authorized capabilities and prints a listing with the names of all users at a site authorized to perform a specific function. Additionally, Local Agency administrators (group administrators) can perform some limited security functions associated with operating a server-based LAN.

The System maintains its security by recording and storing data on authorized users, limiting user access to functions appropriate for that user category, and monitoring unauthorized access to the system. Additionally, the system restricts user access to data only through the application or appropriate ORACLE tools by function.

The local site system described is a menu-driven set of applications requiring several tiers of user access and security. It is assumed that the State Quality Assurance Staff is responsible for

establishing categories of access (guided by State policy), user identification numbers and initial passwords for the various application levels and log on/off procedures.

The system uses unique IDs to identify users with access to the system. The first security layer occurs when a user boots his or her PC and attempts to sign onto the network. If this logon is successful, the user's PC displays the Windows Program Manager with the AIM System icon. To gain access to the application, the user double clicks on the icon and is presented with another logon window, which actually sits in front of the application. The user is given three (3) attempts to successfully logon to the application. If he or she is unsuccessful, a record of unauthorized access is captured in the system and the user is brought back to Windows. If the user is successful, they are brought into the application. To provide this log on/security capability, the system administrator can maintain system security by recording and storing data on authorized users.

Local Agency system administrators are responsible for adding new users utilizing network security and the security functionality within the application. The function to maintain internal security tables is only provided to the Local Agency administrator role.

All passwords stored in the application security or utilized in accessing the system are encrypted.

The network operating system provides the capability to make users change their passwords by periods of time since last password change or on specific dates. This capability can be turned on by the State Systems Administrator at any time and limits the assignment, maintenance and cancellation of operating system passwords to State/Local Administrators.

Monitor Unauthorized Access

The AIM System monitors attempts by users (who have general access to the system) to gain access to specific functions for which they are not authorized according to the capability list described in the previous capability. The System produces a report, upon request, that lists individuals who have attempted to gain unauthorized access to WIC Functions.

The System detects and tracks three different kinds of access:

- Normal access

- Unauthorized access which failed

- Unusual, successful access

All of these accesses are tracked using the network operating system, ORACLE or application level security. The System has this capability at both the Local Agency and State Agency levels. Also, the function of producing these reports is only available at the system administrator level.

In determining the "unusual, successful access," the System determines unusual access against the clinics' hours of operation as defined in the appointment scheduler. (Note: This infers that hours of operation for a clinic are when the doors are open. This issue cuts across functional areas.)

Maintain Record Audit

The System records the user ID and date of creation for all data in all tables in the system. Additionally, any data that is updated has the User ID and date also recorded in a separate column from the creation user ID and date. Only the last person updating the record has their User ID and date recorded, as all previous entries are overwritten.

Limit Unauthorized Access

The AIM System invokes a Windows-based window saver if a terminal goes unused for a set period of time. To get back into the application, the user must enter a User ID and password through a message box facility.

The System also logs off any workstation that has not been utilized for a set period of time. This network operating system administration function automatically logs off the user from the network and application. Any information that was entered but not saved is lost.

Other Security Measures

The System employs a number of system security measures:

- Restricts user access to data only through programs or approved ad hoc tools.

- Restricts user access to data by function. The System includes a recovery and restart procedure for application software in the event of errors.

- All data electronically transmitted by the System is encrypted by the sending station before transmission and decrypted by the receiving station upon receipt of transmission.

Archive System Data

WIC Program requirements stipulate that various types of records be kept for a number of years. To satisfy this requirement while preserving efficient system operation, it is necessary to remove information that is not required for day-to-day processing in the AIM System. Historical WIC data can be stripped from the system and stored off-line (archived) for potential future use.

Archive Historical Data

The AIM System archives historical WIC participant and vendor records according to parameters specified by the State Agency. It is possible to specify different time periods for different types of records since it is important to retain some types of data for longer time periods than others. The System builds a table that informs a user that a record was previously stored in the system and is now located in the system archives. The AIM System can retrieve those files for user access within 24 hours, upon request. Operating procedures are established at Local Agencies and clinics to request retrieval of this information so that participants are not turned away because their files are not available on-line.

As records are archived, an index is created and updated containing the participant identification, name, and date of archival. This indexing allows for selective retrieval from the archive tape by

participant. An archival report is also printed listing the index. This index report is safely stored along with the appropriate archive tape.

Archiving is to be done on a regular basis determined jointly by ADHS, Integris, and CMA. The MicroAge Operations Center performs the actual archival process.

Retrieval of Historical Data

The System provides the capability of retrieving historical data from archive and restoring it. The Operations Center administrator can specify vendors or participants to be retrieved from tape media. Any requested data is transmitted over the wide area network utilizing the end-of-day process for use by the State Agency, Local Agency, or clinic the next day. Participant retrieval not only restores participant data but also information about food packages issued to the participant.

Purge Unnecessary Data

This process is identical to the archive process described above, with the exception that the data is not stored before it is stripped from the System. The State Agency may collect some types of information that are of no use after the period that they are needed online. The System allows this information to be purged completely.

The System Administration function is where purge criteria is defined and purging functions are run. Purging functions are run on an ad hoc basis as system resources become available at the time an archive is requested. Purging is done at both the State and Local Agency servers.

The WIC System purges all data that has been unused for a user-specified length of time. This occurs as a normal part of the archive process.

Maintain Archive Parameters

The system provides defaults for determining the inactive period at which data is to be archived (66 months for participant data, 999 months for vendor data). It is also necessary to provide the capability to change these values on an ad hoc basis. The system allows users to enter these values whenever data is archived.

Administer Backup/Restore

The AIM System provides the WIC Systems Administrator with the ability to administer backup and restore procedures in the most simple and effective method possible.

Provide Central System Backup Capability

Backup functions are provided for the Central database. This function is executable from the menu and has user selectable options that define the content of databases, directories, and files that the system backs up.

On a daily basis, the System backs up the system to tape via the end-of-day process. In addition, the backup process is executable as a separate menu item by the administrator, who can also define the type of backup to perform including full export of the WIC Application Tables, Weekly Backup of Disk Structure, or custom. Each of these backups has a different set of files and directories associated with it. Restoring the backup must be done manually.

Because backup tapes are most likely reused following a father-grandfather rotation, they should not be used for archiving. It is recommended that archive tapes be placed in storage and never reused, as it is the only copy containing particular data.

Provide Local Agency System Backup Capability

Backup procedures at the Local Agency functions in a similar manner to that utilized on the Central server: they are automatically performed via the end-of-day process, but a user selectable backup process is included on the menu at Local agencies.

> **Note: It is the responsibility of users or local administrators to backup their own workstation.**

Administer End of Day

The End of Day process initiates a number of processes and reports for the agency/clinic. The local administrator uses a simple window from which all of these processes are run. These processes cannot be individually run from this area. The window prompts the user for three distinct items to have been completed before the End of Day process is initiated. These are: Verify that the clinic functions are completed for the day, verify that the printers are on and are loaded with paper, and verify that the backup tape has been loaded in the server. Once the user initiates the process, it proceeds automatically, and no user intervention is required from this point forward. The backup and end of day processes proceed during the evening and produce outputs for staff members to review on the following business day.

Process End of Day Activities

The End Of Day (EOD) activities assist in the movement of data throughout the automated WIC System. Additionally, EOD activities backup important data files, and produce status logs to assist the system administration (a complete list is shown below).

Central

Ctrl_sql.log - A list that details by date the participants at each agency, whose records were added, deleted or updated. This includes information regarding the processing of food instruments.
Sql.log - A historic list that details by date the participants at each agency, whose records were added, deleted or updated.
Ec.log - A list that details by date and time that all Central Agency scripts initiated and finished.
Ec_his.log - A historic list that details by date and time that all Central Agency scripts initiated and finished.
Mon_bank.log - A historic log file that details by date and time the scripts are initiated and completed to transfer information back and forth between the Central Database and the Banking Intermediary.
Agcy_01.log - This script details for a single local agency (in this case 01) the table data that was extracted from the agency's base tables, updated at the Central server, then exported from the Central server database.
Agcy_01_his.log - This script is a historic log that details for a single local agency (in this case 01) the table data that was extracted from the agency's base tables, updated at the Central server, then exported from the Central server database.
01_ec4_retrieve.log - This script details that the scripts concerning retrieving and storing

requested archived data at the Central Database have run.

Local Agency

Ea.log - This script details by date and time that outputs at the local agency have printed.
Mon_agcy.log - This is a historic log that details by date and time that connections and file transfers were successful to and from the Central Server database.
Agcy_ctrl.log - A list that details inserts of all new and updated data into the End of Day temporary tables. It also provides information regarding the export of these tables for preparing the zip file to be sent to the Central Server database.
Agcy_sql.log - A list that details participants who have been terminated or experienced a category change during the End of Day process.
Appt_Not.log - Details whether the printing of appointment notices was successful or unsuccessful.
Ctrl_agcy.log - A list that details the transfer of base table, participant, and food instrument data from the Central Server Database to the Agency Server Database.
Agcy_01.log - A historical log that details for the agency the data that was extracted from the agency's base tables and exported to the central server.
EC4_DUAL - This report prints out at each local agency detailing the Participant ID, Name, Birth Date, Category, Address and Phone Number of Participants who are showing a dual enrollment in the AIM system.
Ineligibility Notices - The system prints out a letter for each participant who has been determined ineligible through the end of day process.
Appointment Notices - The system prints out a letter for each participant who is scheduled to have a WIC / CSFP appointment in 14 days.
Appointment Labels - The system generates a mailing label for each Appointment notice letter generated.
CSF Notice to Reapply - The system generates a letter for participants who must reapply for CSF because their eligibility will end in 6 weeks.

Administer External System Interfaces

The AIM System must interface with other systems by providing data for them. One of the functions of this system is to provide data to the Centers for Disease Control and Prevention (CDC) and ABT Associates regarding WIC participant Characteristics, Pregnancy Nutrition Surveillance Data, and Pediatric Nutrition Surveillance Data. This information is transferred to the CDC and ABT Associates in methods prescribed by Federal Requirements for each of them, and are further described below. Each of the reporting interfaces has their own window to generate the specific reporting file of information.

Generate Participant Characteristics Information

The Participant Characteristics Report File is generated to meet Federal reporting requirements, and is transmitted via magnetic tape. The user produces the report (usually in April) by entering the month for which they wish to generate the report. This report is then generated to the tape and can be submitted to ABT Associates (a federal contractor) for final submission to the CDC.

Generate Pediatric Nutrition Surveillance Information

The Pediatric Nutrition Surveillance Report (PEDS) is generated to meet federally required reporting regarding pediatric participant characteristics. This information is then output to a file for input to the EPI Info System, or written to magnetic tape for submission to the CDC. The Systems Administrator must select which output type s/he desires, and if it is for the EPI Info System, s/he must enter the filename to be created. Once the output is selected, the user must enter the month for which the report will be generated. This is all done from one window.

Generate Pregnancy Nutrition Surveillance Information

The Pregnancy Nutrition Surveillance Information Report (PNSS) is generated to meet federally required reporting regarding pregnant participant characteristics. This information is then output to a file for input to the EPI Info System, or written to magnetic tape for submission to the CDC. The Systems Administrator must select which output type s/he desires, and if it is for the EPI Info System, s/he must enter the filename to be created. Once the output is selected, the user must enter the quarter for which the report will be generated. This is all done from one window.

Administer Data Transfer Between Outreach Clinics and Local Agencies

When an Outreach Clinic is held, it is necessary to load data from the Local Agency Database to the Outreach Clinic laptop computer. This is done through a process commonly referred to as "checking out" the data. This process protects participant data from corruption/lack of synchronization, and allows the clinic to operate as if it had a database server with it. Once the clinic has been completed, the updated data can then be "checked in" to the Local Agency database from the laptop. This data is then updated to the State Agency's database. The system allows the user to load data necessary to support mobile laptop functionality, and to enable the Local Agency to perform outreach clinics at remote sites. This functionality has not been finalized to date. Therefore this section of capabilities needs to be updated when the details of that function are completed.

Provide Management Reports

The AIM System provides a time management report on the security aspects of the application. These reports are provided to assist site administrators in maintaining security.

Expired Passwords

The AIM System monitors and lists all users whose password has expired. The purpose of this is for the administrator to consider deleting the user since the account is not accessible. Unused accounts may propose a security risk.

Pending Certification Records

This report details those participants entered in the AIM System who have begun the certification process, but have not been issued food instruments. This report does not include exclusively breastfed infants.

System Access

The AIM System provides a listing of all accesses to the applications that were denied, and the reason for the denial.

WIC Active and Inactive Roles

The AIM System provides a listing of WIC roles and references these roles as "Active" or "Inactive." This gives the administration a "quick view" capability as to which privileges associated with these roles are entered.

WIC Role Authorities

The purpose of this report is to provide the system administrator with a breakdown of the currently established roles, the tables that each role has access to, and the privileges of each table.

WIC User Directory

The purpose of this report is to provide a listing of all current WIC users, their associated roles, and their password expiration dates. This provides the system administration, and any required supervisors, with the ability to create and view a hard copy report of all users.

System Administration Main Menu

When clicking on the System Administration button from the AIM System Master Menu, the following window is displayed:

Description of System Administration Functions
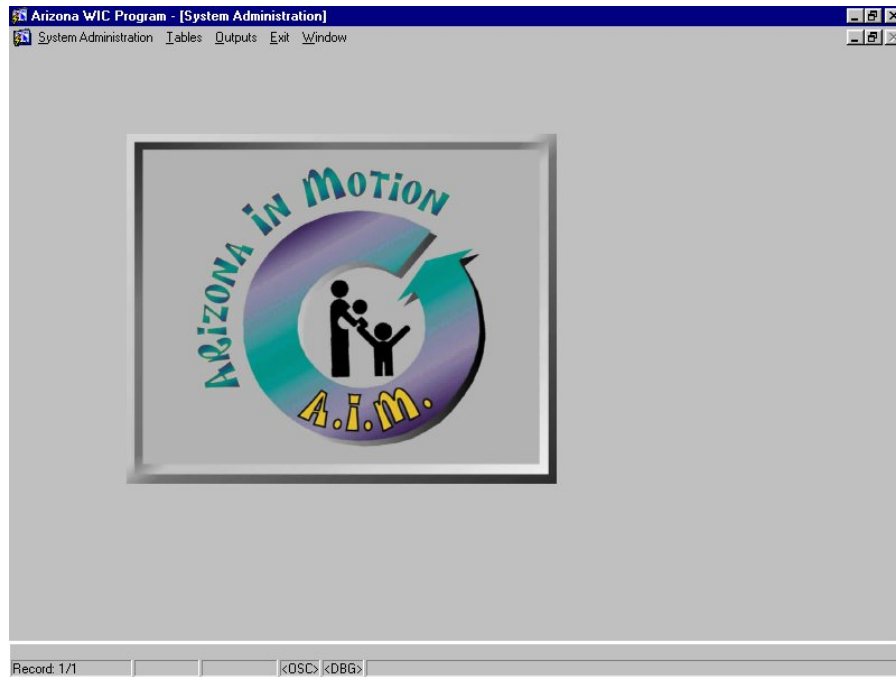
Figure 1 – System Administration Splash Screen

Performing a Backup

To Perform a Backup:

1. Backup must be performed at the Server workstation.
2. Click System Administration on the menu bar.
3. Click Backup as shown below:
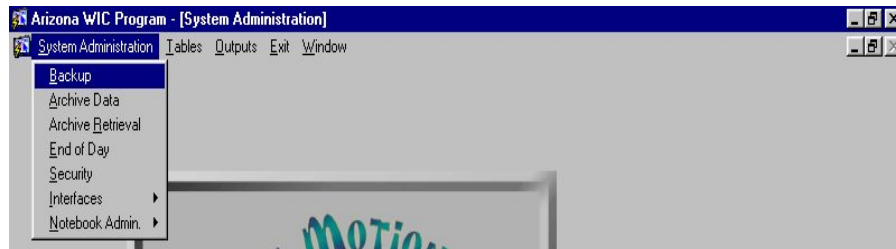
The Backup window is displayed:
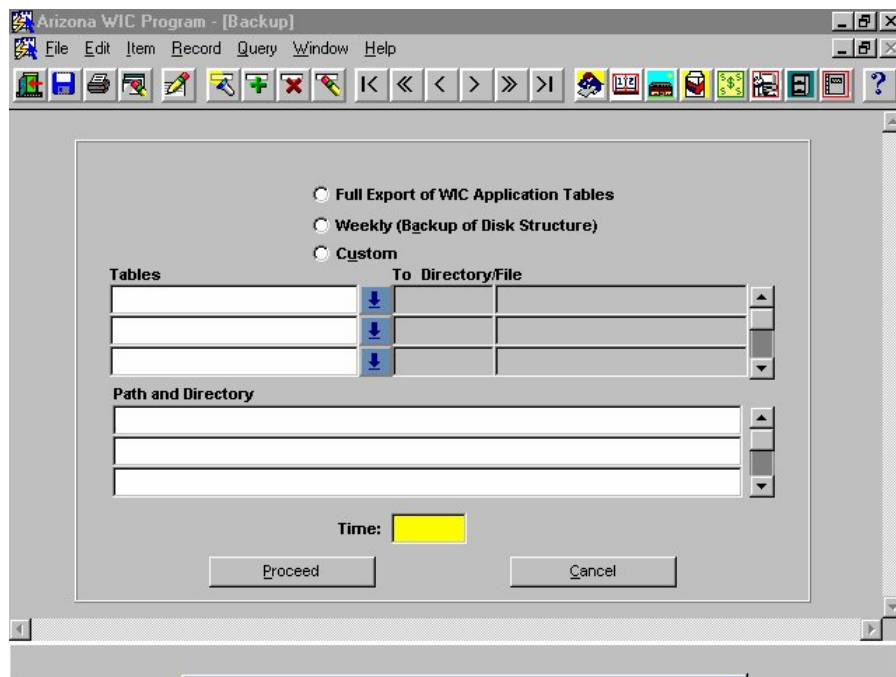
Figure 2 - Backup

Perform Backup

1. Select whether you want a Full Export, Weekly or Custom backup by clicking once on the radio button next to that type of backup.
2. TAB to the Time field. Then type the time you want the backup processing to begin, using following format: HH:MM AM or HH:MM PM.
3. Insert the back-up tape into the tape drive.
4. Click the Proceed push button to initiate the Backup process, or click the Cancel push button to exit the window.

Perform a Custom Backup

1. Select the Custom backup by clicking once on the radio button next to the Custom field.
2. The System displays the To Directory/File fields with the designated directory location and file name to which the selected application Tables backup files are to be written.
3. Tab to the Path and Directory field and enter the server file directory path(s) which are to be backed-up.
4. TAB to the Time field, and enter the time you want the backup processing to begin, using the following format: HH:MM AM or HH:MM PM.
5. Insert the back-up tape into the tape drive.
6. Click the Proceed push button to initiate the Backup process, or click the Cancel push button to exit the window.

Figure 2 - Backup

Fields

Tables - Enter tables to be backed up (custom selection only). This field contains a list of values that is selected and maintained by the user. This field is optional.
To Directory/File - The System-designated directory location and file name to which the selected application table's backup file(s) are to be written. This field is display only.
Path and Directory - This field allows the user to enter the server file directory paths to be backed up in a custom backup. This field is optional.
Time - The time of the day that the system backup is to begin. This field is mandatory and must be entered when the user chooses to schedule the backup for a later time. The time entered must be in the future. This field defaults to 5 minutes from the current System time.

Radio Button(s)

Full Export of WIC Application Tables - When selected, a backup of all the base tables and participant tables in the AIM application is performed.
Weekly - When selected, a backup of all files resident on the application server, including ORACLE System files is performed.
Custom - When this button is selected, the user may choose what tables and files to back up.
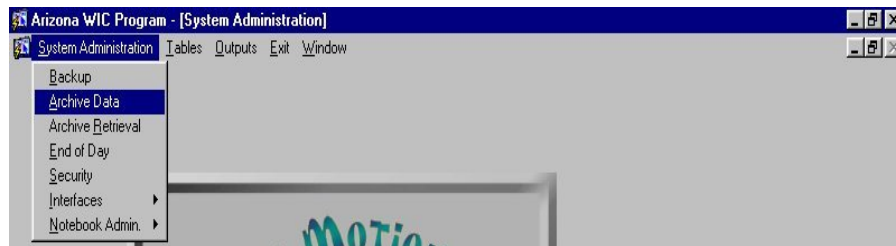
Push Button(s)

Proceed - Click on this button to initiate the backup process.
Cancel - Click on this button to cancel/exit the window.

Archiving Data

To initiate Archive Processing:

1. Click System Administration from the System Administration main menu.
2. Click Archive Data as shown below:

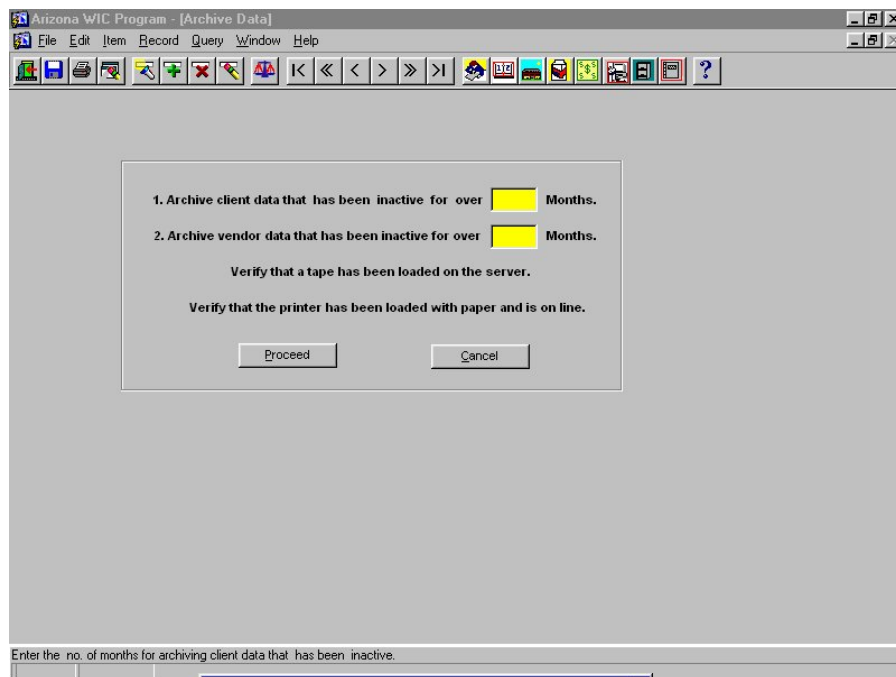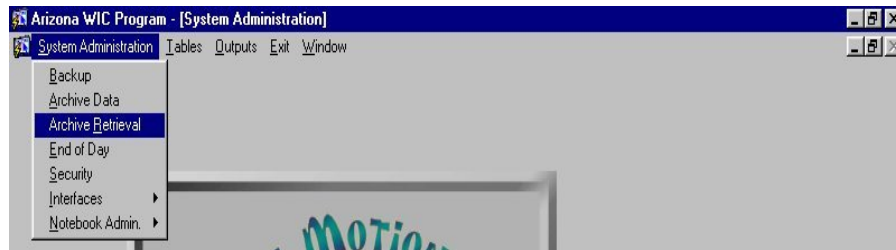
The Archive Data window is displayed:

Figure 3 – Archive Data

Archive Participant and/or Vendor Data

1. To archive participant data, click once in the field following the text in item number 1.
2. Enter the number of months of client inactivity you want to archive (usually 36 months).
3. To archive vendor data, click once in the field following the text in item number 2.
4. Enter the number for months of vendor inactivity you want to archive. The default is 999 months.
5. Load a tape into the server.
6. Load the printer with paper and verify that the printer is online.
7. Click the Proceed button to initiate the archive process or click the Cancel button to exit the

window without initiating the archive process.

Figure 3 – Archive Data

Fields

The age, in months, of inactive participant records to be archived. Any inactive participant and participant related records of that age or older will be archived. This field is mandatory.
The age, in months, of inactive vendor records to be archived. Any inactive vendor records of that age or older will be archived. This field is mandatory.

Push Button(s)

Proceed - Click on this button to initiate the archive process.
Cancel - Click on this button to cancel/exit the Window.

Perform Archive Retrieval

To initiate Archive Retrieval:

1. Click System Administration on the System Administration main menu.
2. Click Archive Retrieval as shown below:

The Archive Retrieval window is displayed:

Figure 4 – Archive Retrieval

Vendor Archive Retrieval

1. Archive Retrieval is a function performed by the Operations Center.
2. To retrieve vendor data, enter either the Vendor ID or the Vendor Name in the appropriate field. Press the F8 key or click the Query icon to execute the query.
3. Verify that the data shown is for the Vendor to be retrieved. Click the Select checkbox next to the vendor data in the display section.
4. Click the Proceed push button to initiate the retrieval process during the end-of-day process or click the Cancel push button to exit the window without initiating the retrieval process.

Participant Archive Retrieval

1. To retrieve participant data, enter either the Client. ID, Last Name, First Name, Local Agency or Clinic in the appropriate field. Press the F8 key or click the Query icon to execute the query.
2. Verify that the data shown is for the Client(s) to be retrieved. Click the Select checkbox(es) next to the participant data in the display section.
3. Click the Proceed push button to initiate the retrieval process during the end-of-day process or click the Cancel push button to exit the window without initiating the retrieval process.

Figure 4 – Archive Retrieval

Fields

The following fields are used as parameters that determine which vendors or clients are shown in the scrollable blocks of the window.

Vendor ID - The identification associated with the vendor data to be restored from archive files. This field is only entered if vendor data is to be retrieved by searching for a specific vendor ID.
Vendor Name - The name of the vendor retail outlet as it was captured during the authorization process. This field is only entered if vendor data is to be retrieved utilizing the outlet (vendor) name.
Client ID - The identification associated with the participant data to be restored from archive files. This field is only entered if the client data is to be retrieved utilizing a specific Client ID.
Last Name - The last name of a client who may need to be retrieved from archive. This field is only entered if the client data is to be retrieved utilizing a specified name.
First Name - The first name of a client who may need to be retrieved from archive. This field is only entered if the client is to be retrieved utilizing a specified name.
Local Agency - The Local Agency of the client(s) who may need to be retrieved from archive. This field is only entered if the client is to be retrieved utilized the specified Local Agency to receive WIC services.
Clinic - The Clinic of the client(s) who may need to be retrieved from archive. This field is only entered if the client(s) to be retrieved utilized the specified Clinic to receive WIC services.

The following fields represent the results of entered parameter values:

Vendor Name - The name of the vendor retail outlet as it was captured during the authorization process. This field is display only.
Vendor Code - The identification number associated with the vendor name returned. This field is display only.
Archive Date - The date that this vendor's information was placed into archival storage. This field is display only.
Last Name - The last name of a participant who may need to be retrieved from archive. This field is display only.
First Name - The first name of a participant who may need to be retrieved from archive. This field is display only.
MI 1 - The first middle initial of a client who may need to be retrieved from archive. This field is

display only.

MI 2 - The second middle initial of a client who may need to be retrieved from archive. This field is display only.

Client ID - The identification of a client who may need to be retrieved from archive. This field is display only.

Archive Date - The date that this client's information was placed into archival storage. This field is display only.

Push Button(s)

Proceed - Click this button to initiate the archive retrieval.
Cancel - Click this button to cancel/exit this window.

Check Box(es)

Select (Vendor) - "X" by clicking on the box to select desired vendor retrieval parameters.
Select (Client) - "X" by clicking on the box to select desired participant retrieval parameters.

Initiating End of Day Processing

To Initiate End of Day Processing:

1. End-of-Day must be performed at the Server workstation.
2. Click System Administration on the System Administration main menu.
3. Click End of Day as shown below:
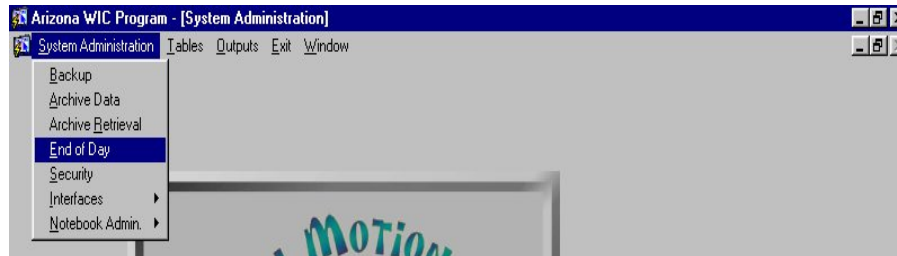
The End of Day window is displayed:
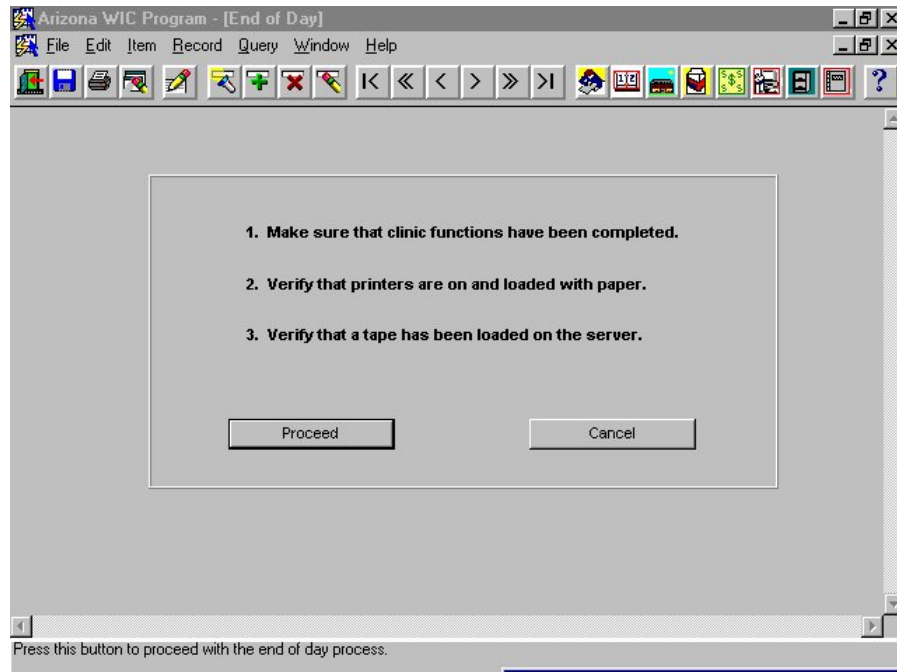
Figure 5 – End of Day

Initiate the End-of-Day Processing Procedures

1. Perform steps 1-3 in the End of Day window.
2. Click the Proceed push button to begin the End-of-Day processing, or click the Cancel push button to exit the window.

Figure 5 – End of Day

Push Button(s)

Proceed - Click on this button to initiate the End-of-Day processing.
Cancel - Click on this button to cancel/exit the window.

Maintaining Security

To Maintain Security:

1. Click System Administration on the System Administration main menu.
2. Click Security as shown below:
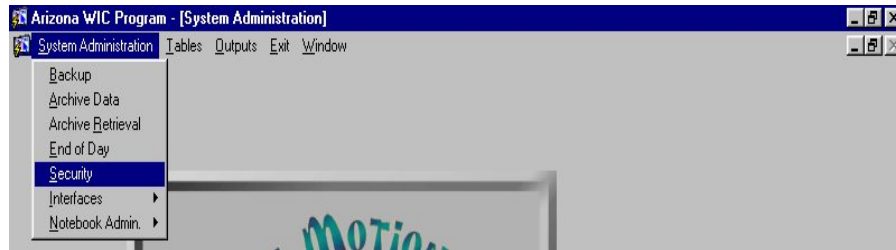
The Security window is displayed:
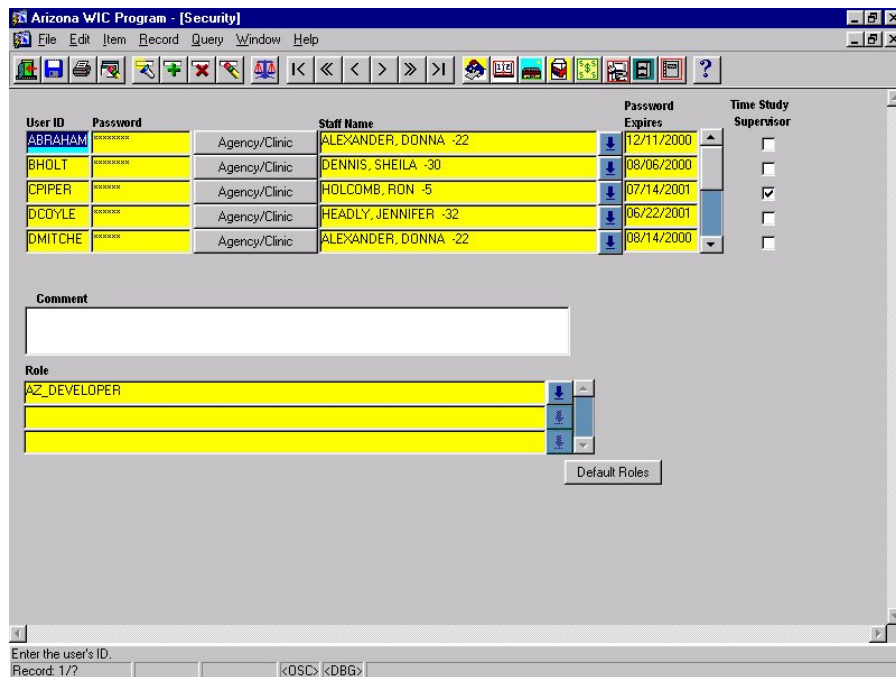
Figure 6 - Security

Add a WIC User and Assign a Role

1. Enter the User ID for the new user. The User ID can contain up to eight alphanumeric characters.
2. TAB to the Password field and enter the password for this user. The password must be four to ten alphanumeric characters. No other characters are allowed. The system shows an asterisk (*) for every character because it automatically encrypts the password entered. This password is just for the new user to initially sign-on to the System. They are required to change their password the first time they log on to the AIM System.
3. TAB off the Password field and the System displays the Password Verification pop-up window.
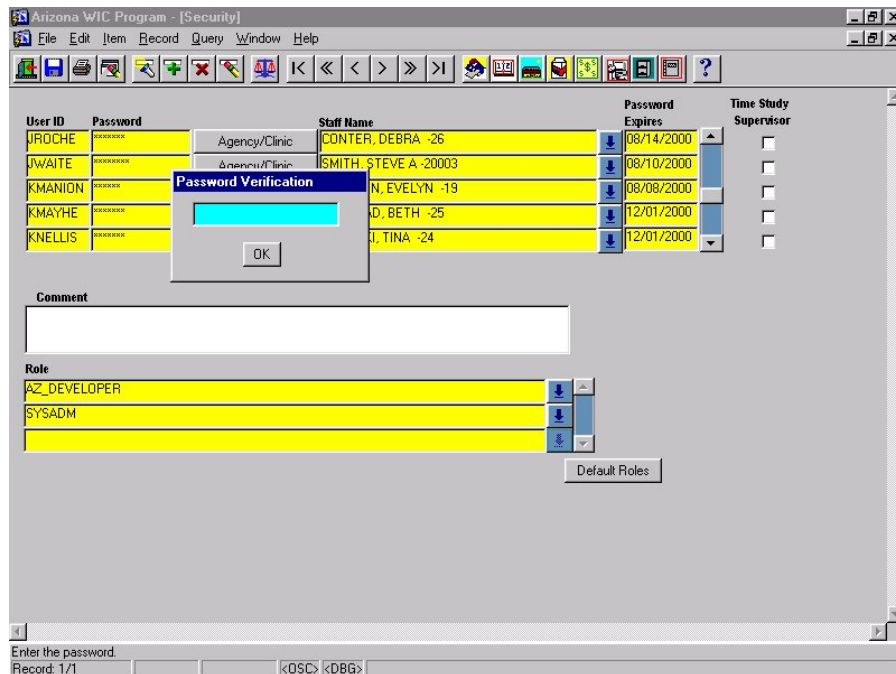
Figure 7 - Security (Password Verification Pop-Up)

4. Re-enter the same Password in the Password Verification field.
5. Click the OK button to close the pop-up and return to the Security window.
6. TAB to the Staff Name field and select the staff person's name from the list of values.
7. TAB to the Password Expires field. The System defaults this field to 8 calendar days from the date the password is first assigned. It may be overwritten within one week, if needed.
8. TAB to the Time Study Supervisor checkbox and mark as checked, if the user is a Time Study Supervisor.
9. Click the Agency push button to display the Agency pop-up window.
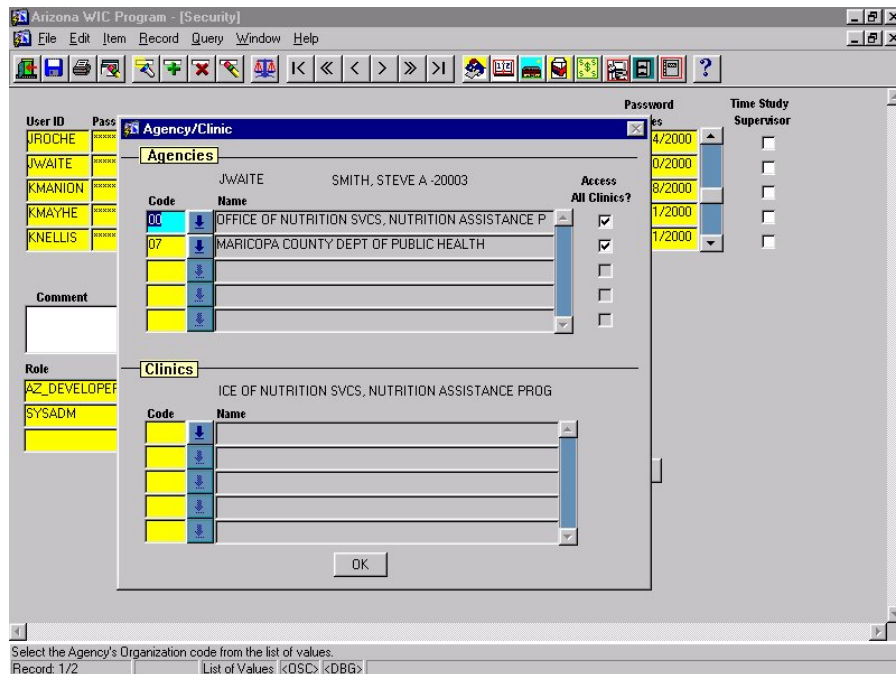
Figure 8 - Security (Agency Pop-Up)

10. Click the Code list of values button and select the Agency with which to associate this user. Repeat for all clinics and Local Agencies for which this staff person is to be given access to the AIM System.
11. Click the OK button to close the pop-up and return to the Security window.
12. TAB to the Comment field and enter any applicable comments, if desired.
13. TAB to the Role field, and select the user's security role(s).
14. Click the Default Roles push button. The system displays the message "Do you want to change default roles to the user <username>?"
15. Click the No push button to close the prompt and return to the Security window. The System does not save any of the user's granted security roles in this situation.
16. Click the Yes push button to proceed to the Granted Roles pop-up window.
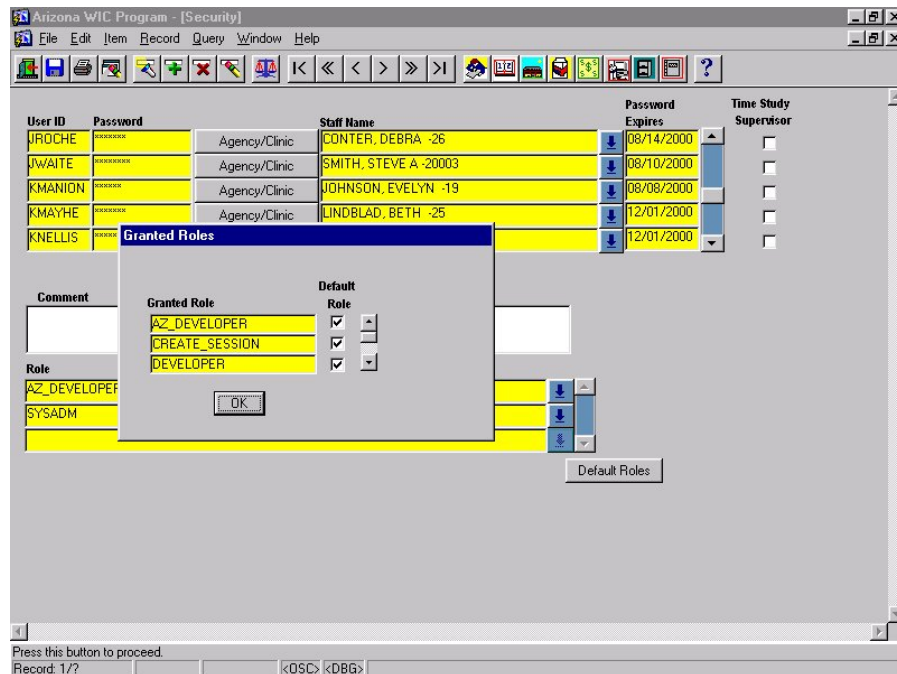
Figure 9 - Security (Granted Roles Pop-Up)

17. The Granted Role field displays the role(s) that are to be associated with this particular User ID. A role appears in this field if it is a basic AIM System role or if it has been selected in the Role field(s) of the Security window.
18. Check the Default Role checkbox for all Granted Roles this user is to be allowed to perform.
19. Click the OK button to return to the Security window.
20. Click the Save icon.
21. The System displays a pop-up window indicating: "Transaction Completed."
22. Click the OK button and a new WIC User has successfully been added into the system.

Update a WIC User

There are several methods to update a user. One way is to change their password. Another way is to modify the agencies to which the user can logon.

> **Note: If the user logs on at the State level, they are able to change user roles so that any user is able to log on to any agency. If the user logs on at a specific agency, s/he is only able to add that agency to any of the users.**

To Change Password

1. Click the Password field you wish to update.
2. Remove the old password using the backspace key or by selecting Item > Clear from the pull down menu on the tool bar.
3. Type in the new Password.
4. Press the Enter or TAB key to display the Password Verification pop-up.
5. Complete as previously instructed.
6. Click the Save icon on the toolbar to save the data.

To modify agency access

1. Click the Agency push button corresponding to the user to update. The System displays the Agency pop-up window (as previously described in this section).
2. To remove an agency/clinic for this user, click the Code field of the agency. Then click the Remove Record icon.
3. To add more agencies for this user, with the cursor in the Code field, click the Insert Record icon on the toolbar. Then, select the additional agency/clinic from the list of values.
4. Click the OK button to return to the Security window.
5. Click the Save icon. The system displays a pop-up window indicating: "Transaction Completed."
6. Click the OK button.

Delete a WIC User

1. Click the Enter Query icon.
2. Enter the User ID of the WIC User to delete, and then press the F8 key to execute the query.
3. The system automatically populates the remaining fields on the window with the current data for that User ID. Verify that this is the correct record to delete.
4. Click the Remove Record icon, the AIM System automatically deletes that User security information and displays the message, "Transaction completed."
5. Click the OK button to return to the Security window.

To add a Role

1. With the cursor in the Role field, click the Insert Record icon on the toolbar. Then, select the additional role from the list of values.
2. Click the Default Roles push button and update the roles as previously described.
3. Click the Save icon on the toolbar to save the changes.

Delete a Role

1. With the cursor in the Role field you want to delete, click the Remove Record icon on the toolbar.
2. The AIM System automatically deletes that Role and displays the message, "Transaction completed."
3. Click the OK button to return to the Security window.

Figure 6 - Security

Fields

User ID - The AIM System user ID assigned to the user. The User ID is allowed to be up to eight alphanumeric characters. This field is mandatory.
Password - The encrypted Oracle password associated with the User ID. The password is allowed to be from four to eight alphanumeric characters. This field is mandatory.
Staff Name - The staff member associated with the User ID/password combination is selected from the list of values. This field is mandatory.
Password Expires - The date the password associated with the User ID expires. The date defaults to 45 calendar days from the current system date but the user may overwrite. This field is mandatory.

Comment - The user may enter comments associated with this staff member's User ID and Password. This field is optional.

Role - These represent pre-defined groups of user privileges to perform certain actions. A user can be assigned to one or more roles selected from the list of values. This field is mandatory.

Check Box(es)

Time Study Supervisor - Check this check box if the user is a Time Study Supervisor.

Push Button(s)

Agency - Clicking this push button allows the user to display the Security-Agency popup window in which the user associates an agency/agencies with the staff member.

Default Roles - Clicking this push button allows the user to display the Security – Granted Roles popup window in which the user can assign or change the granted roles assigned the user ID.

Figure 7 - Security (Password Verification Pop-Up)

Fields

Password Verification - The encrypted Oracle password associated with the User ID. Re-entry of the password is mandatory to "double-check" the accuracy of the first entry.

Push Buttons

OK - Closes the pop-up window and returns the user to the Security window.

Figure 8 - Security (Agency Pop-Up)

Fields

Code - The numeric identifier for the State Agency, Local Agency, or Clinic to which the user is associated is selected from the list of values. This field is mandatory

Name - The name of the organizational unit associated with the selected Code. This field is display only.

Push Buttons

OK - Closes the pop-up window and returns the user to the Security window.

Checkboxes

Access all Clinics -

Figure 9 - Security (Granted Roles Pop-Up)

Fields

Granted roles - The access roles assigned to the user. This field is mandatory.

Check Box(es)

Default role - The checkbox must be marked to activate the role displayed in the corresponding Granted Role field. If the user fails to check the box next to a role, the role is not applied to the functions allowed by the User ID.

Push Button

OK - Clicking this button closes the Granted Roles popup and returns the user to the Security window.

Participant Characteristics

To Initiate Participant Characteristics:

1. Click Interfaces on the System Administration main menu.
2. Click Participant Characteristics as shown below:
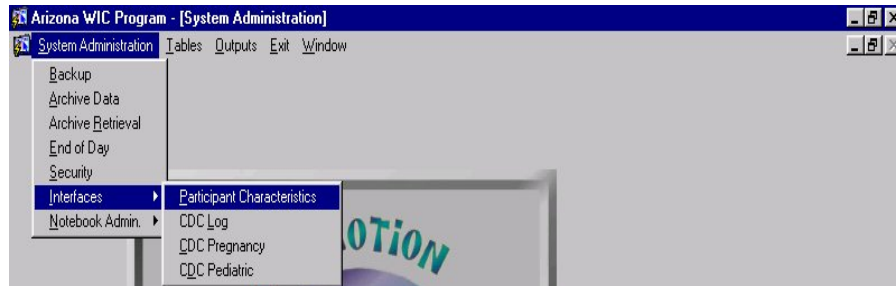
The Participant Characteristics window is displayed:
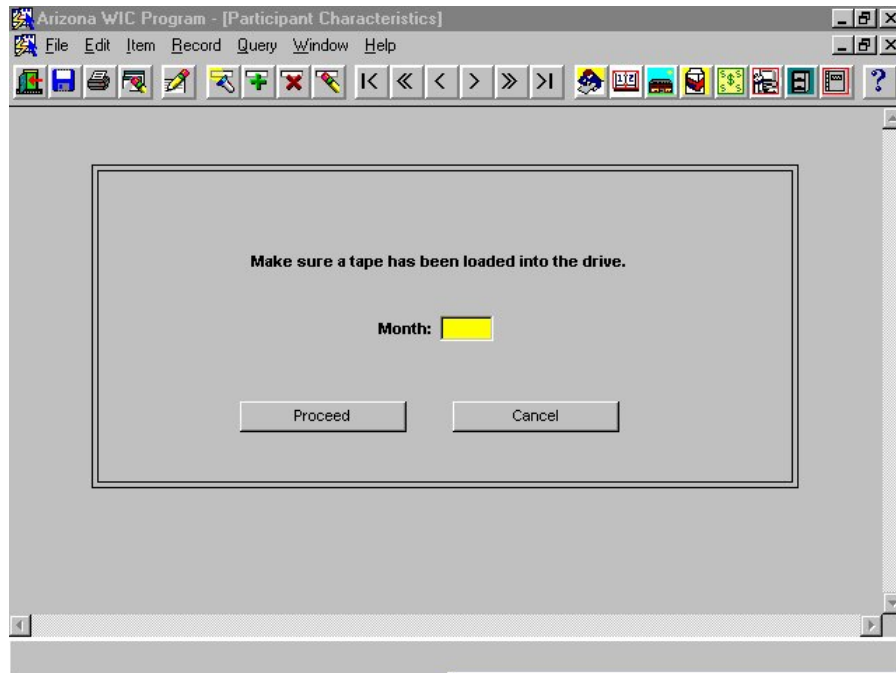
Figure 10 - Participant Characteristics

Initiate Participant Characteristics Tape

1. Make sure that a tape is loaded into the server drive.
2. Enter the Month for which the participant characteristics are desired.
3. Click the Proceed push button to initiate the creation of the Participant Characteristics tape, or click the Cancel push button to exit the window without creating the tape.

Figure 10 - Participant Characteristics

Fields

Month - A mandatory field entered by the user that defines the month that the "snapshot" of participant data is captured. This is usually April.

Push Button(s)

Proceed - Clicking this push button initiates the creation of the participant characteristics tape.
Cancel - Clicking this push button to cancel/exit the Window.

Updating a CDC / Participant Characteristics File Transmission Log

To Produce a CDC/Participant Characteristics File Transmission Log:

1. Click Interfaces on the System Administration main menu.
2. Click CDC Log as shown below:
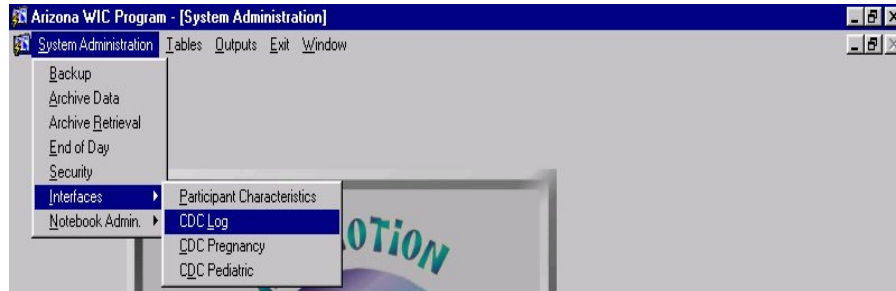
The CDC / Participant Characteristics File Transmission Log window is displayed:

Figure 11 - CDC / Participant Characteristic Transmission Log

Initiate CDC/Participant Characteristic Transmission Log

1. With the cursor in the Run Time Period field, enter the year and quarter indicating the time frame which the file covers.
2. TAB to the Trans. Date field and enter the date the file was submitted to the CDC or USDA.
3. TAB to the Trans. Type field and select the type of file sent from the list of values.
4. TAB to the # records sent field and enter the number of records included in the file transmission.

5. TAB to the Filename field and enter the name of the file.
6. TAB to Sender and enter the last and first names of the staff member responsible for transmission of this file to the CDC or USDA.

Figure 11 - CDC / Participant Characteristic Transmission Log

Fields

Run Time Period - The user-entered year and quarter indicating the time frame the content of the file covers. This field is optional.
Trans. Date - The user-entered date the file was submitted electronically or via CD to the CDC or USDA. This field is optional.
Trans. Type - The user-selected type of file sent: Pregnancy, Pediatric or Participant Characteristics. This field is optional.
 # Records sent - The user-entered number of records included in the file transmission recorded here. This field is optional.
Filename - The user-entered name of the electronic file generated by the user running the CDC Pediatric, CDC Pregnancy, or Participant Characteristics window. This filename is system generated, but is user-entered here. This field is optional.
Sender - The Last name, First Name of the staff member responsible for transmission/submission of this file to the CDC or USDA for reporting. This field is optional.
Comment - The user may enter comments concerning the transmission record entered here. This field is optional.

CDC Pregnancy

To produce a CDC Pregnancy file:

1. Click Interfaces on the System Administration main menu.
2. Click CDC Pregnancy as shown below:
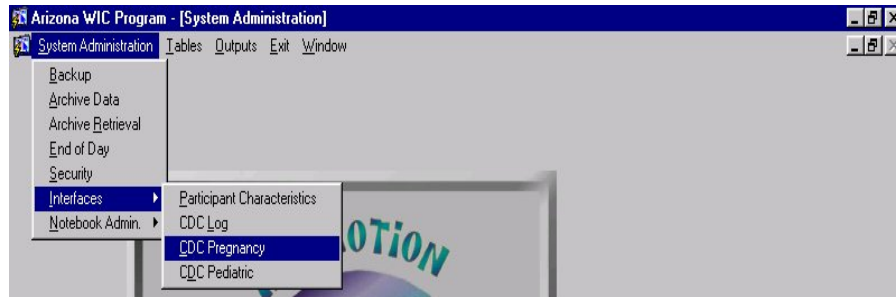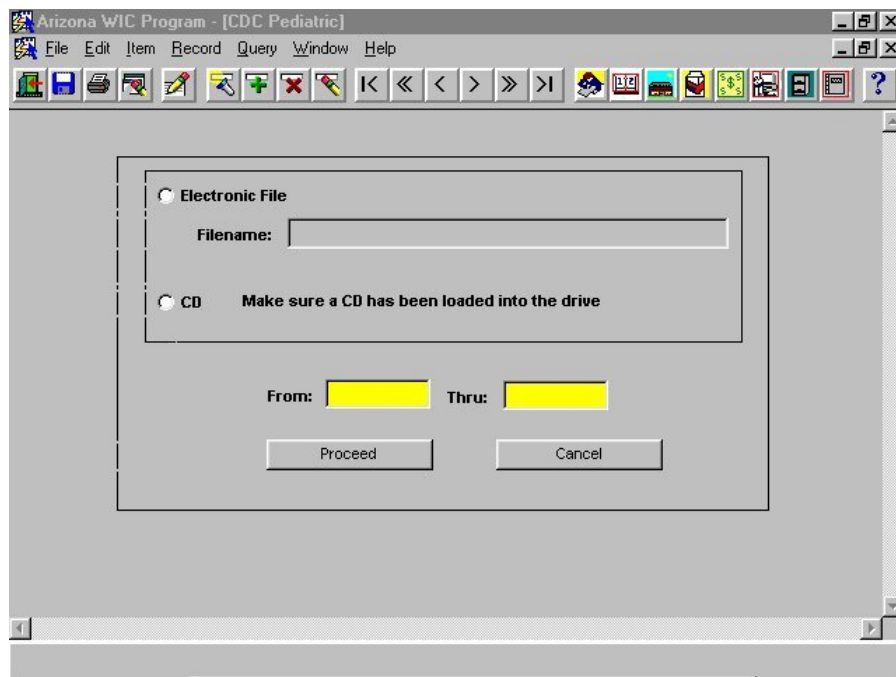

The CDC Pregnancy window is displayed:
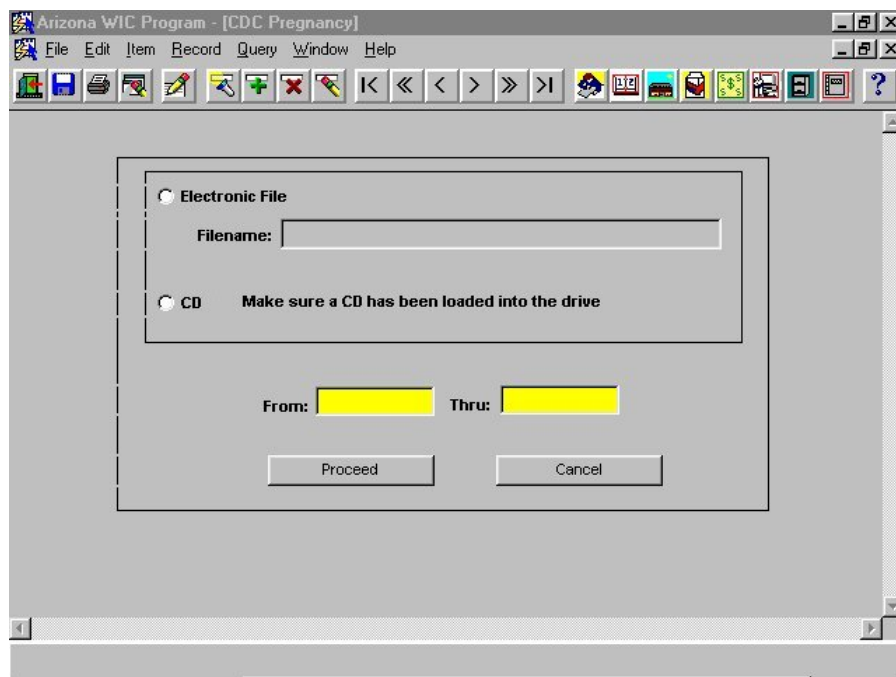
Figure 12 - CDC Pregnancy

Initiate CDC Pregnancy file as Electronic File

1. Select the Electronic File radio button.
2. Enter the Filename for the file being created.
3. TAB to the From and Thru fields and enter the date range upon which the file is to report.
4. Click the Proceed push button to initiate the creation of the CDC Pregnancy file or click the Cancel push button to exit the window without creating the file.

Initiate CDC Pregnancy File on CD

1. Select the CD radio button.
2. Enter the Filename for the file being created.
3. TAB to the From and Thru fields and enter the date range upon which the file is to report.
4. Click the Proceed push button to initiate the creation of the CDC Pregnancy file or click the Cancel push button to exit the window without creating the file.

Figure 12 - CDC Pregnancy

Fields

Filename - Name of the file to be created. This field is optional.
From/Thru - The range of dates upon which the report will filter data, excluding information not falling within the specified range. These fields are mandatory.

Radio Button(s)

Electronic File - The user selects this button to create an electronic version of the report for storage on the network server.
CD - The user selects this button to create a CD on which to store the report being generated for the selected time period. This CD will then be sent to the CDC.

Push Button(s)

Proceed - Click this button to initiate the creation of the CDC pregnancy file or CD.
Cancel - Click this button to cancel the process and exit the window.

Producing a CDC Pediatric File

To Produce a CDC Pediatric File:

1. Click Interfaces on the System Administration main menu.
2. Click CDC Pediatric as shown below:
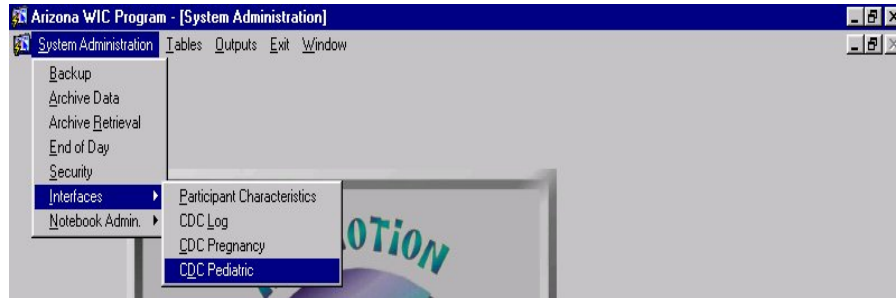
The CDC Pediatric window is displayed:

Figure 13 - CDC Pediatric

Initiate CDC Pediatric file as Electronic File

1. Select the Electronic File radio button.
2. Enter the Filename for the file being created.
3. TAB to the From and Thru fields and enter the date range upon which the file is to report.
4. Click the Proceed push button to initiate the creation of the CDC Pediatric file or click the

Cancel push button to exit the window without creating the file.

Initiate CDC Pediatric File on CD

1. Select the CD radio button.
2. Enter the Filename for the file being created.
3. TAB to the From and Thru fields and enter the date range upon which the file is to report.
4. Click the Proceed push button to initiate the creation of the CDC Pediatric file or click the Cancel push button to exit the window without creating the file.

Figure 13 - CDC Pediatric

Fields

Filename - Name of the file to be created. This field is optional.
From/Thru - The range of dates upon which the report will filter data, excluding information not falling within the specified range. These fields are mandatory.

Radio Button(s)

Electronic File - The user selects this button to create an electronic version of the report for storage on the network server.
CD - The user selects this button to create a CD to store the report being generated for the selected time period. This CD is then sent to the CDC.

Push Button(s)

Proceed - Click this button to initiate the creation of the CDC pregnancy file or CD.
Cancel - Click this button to cancel the file creation and exit the window.

Maintaining CDC Log

To Maintain CDC Log:

1. Click Tables on the System Administration main menu.
2. Click CDC Log as shown:

<p style="text-align:center; color:red">Screen shot not available</p>

The Maintain CDC Log window is displayed:

<p style="text-align:center; color:red">Screen shot not available</p>

Figure 14 - Maintain CDC Log

Add CDC information

Information not currently available

Update a CDC information

Information not currently available

Delete CDC Information

Information not currently available

Figure 14 - Maintain CDC Log

Fields

Information not currently available

Maintaining Contact Methods

To Maintain Contact Methods:

1. Click Tables on the System Administration main menu.
2. Click Contact Methods as shown below:


The Maintain Contact Methods window is displayed:
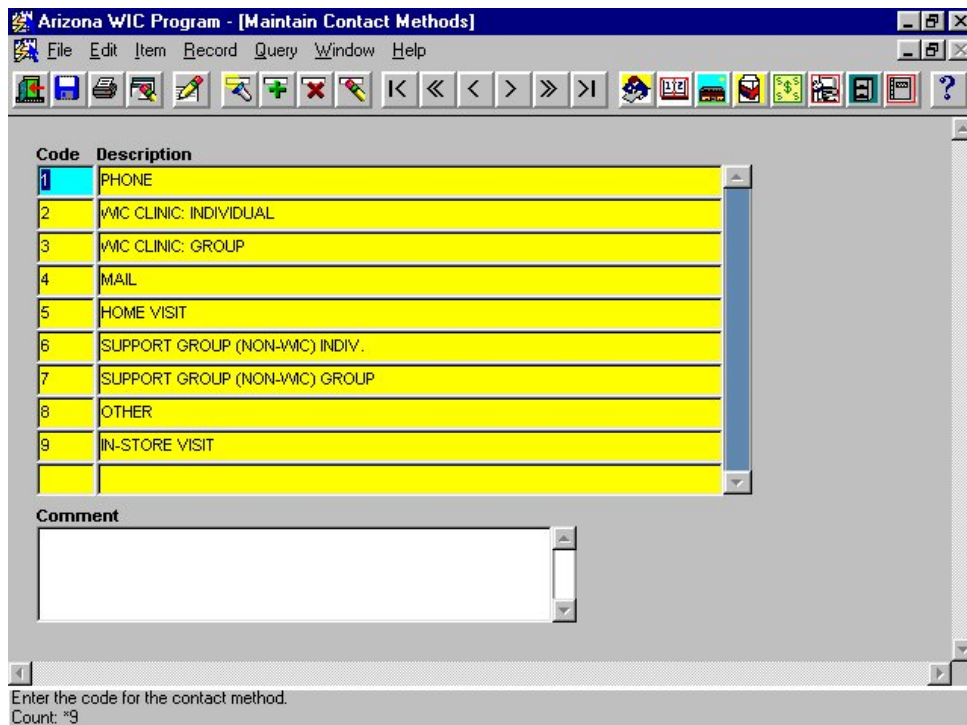
Figure 15 - Maintain Contact Methods

Add a Contact Method

1. The System defaults the cursor to highlight the Code number under the first entry in the Code field. The System also displays the Description and any existing Comments for that Contact Method.
2. Click the Insert Record icon on the toolbar. The System creates a blank space under the Code and Description fields to add a new Contact Method.
3. In the Code field enter a number for the new Contact Method. If the code you choose is already in use for another Contact Method, the System displays a pop-up window indicating:

"Row already exists with the same Code." Click the OK button, delete the Code number inserted, and enter a different number.

4. TAB to the Description field and enter the description of the new Contact Method.
5. TAB to the Comment field and enter any appropriate comments.
6. Click the Save icon.
7. The system displays a popup window indicating: "Transaction Completed."
8. Click the OK button.

Update a Contact Method

1. Press the F7 key or click the Query icon.
2. The System automatically clears all of the fields.
3. The cursor moves to the first blank under the Code fields.
4. In the appropriate field, enter either the Code or the Description of the Contact Method being updated.
5. Press the F8 key or the Query icon to execute the query.
6. The System displays any known data corresponding to this Contact Method.
7. Verify that the information displayed is for the Contact Method being updated.
8. Update the Description or Comment as needed. (*Note: The system does not allow updates to the Code itself. If attempted, the system indicates: "Field is protected against update."*)
9. Click the Save icon. The system displays a popup message indicating: "Transaction Completed."
10. Click the OK button.

Delete a Contact Method

1. Press the F7 key or click the Query icon.
2. The System automatically clears all of the fields.
3. The cursor moves to the first blank under the Code fields.
4. In the appropriate field, enter either the Code or the Description of the Contact Method being deleted.
5. Press the F8 key or the Query icon to execute the query.
6. The System displays any known data corresponding to this Contact Method.
7. Verify that the information displayed is for the Contact Method being deleted.
8. Click the Remove Record icon. The System deletes the record from the window, leaving the fields blank.
9. Click the Save icon. The system displays a popup message indicating: "Transaction Completed."
10. Click the OK button.
11. To verify that the deletion has worked successfully, repeat steps 1-5 above. If the deletion was successful, after pressing the F8 key the system displays the following error message in a popup box: "Query caused no records to be retrieved. Re-enter."

Figure 15 - Maintain Contact Methods

Fields

Code - User-entered numeric code associated with a contact method. This field is mandatory.
Description - A description of the contact method associated with the code. This field is mandatory.

Comment - Any free form text that the user desires to enter concerning the contact method. This field is optional.

Maintaining Contact Titles

To Maintain Contact Titles:

1. Click Tables on the System Administration main menu.
2. Click Contact Titles as shown below:
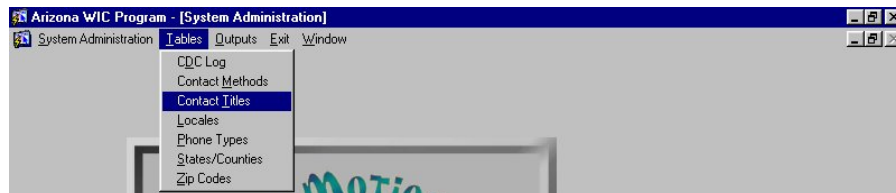
The Maintain Contact Titles window is displayed:
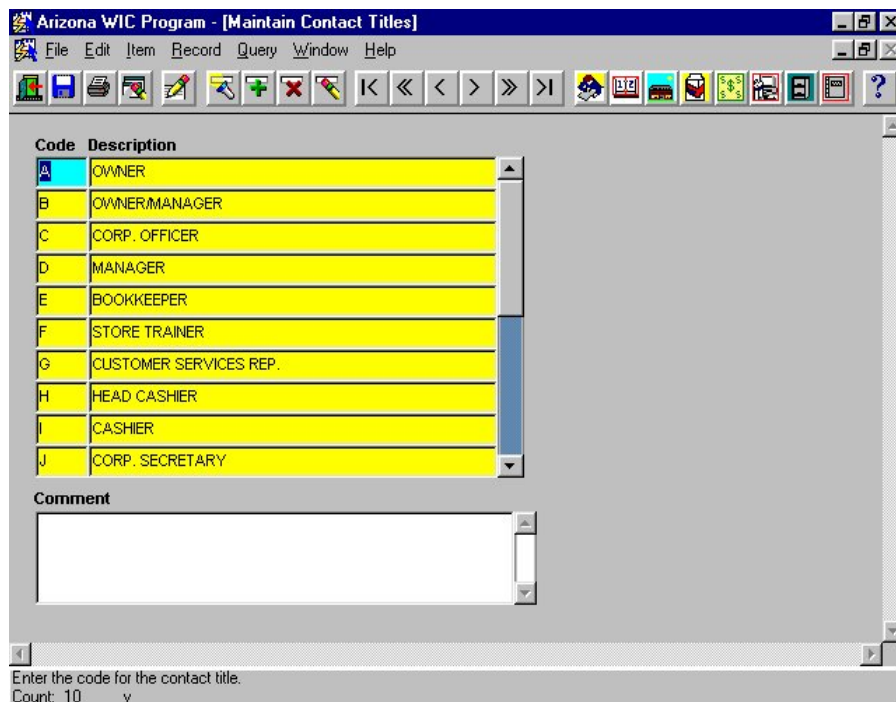
Figure 16 - Maintain Contact Titles

Add a Contact Title

1. The system defaults the cursor to highlight the code under the first entry in the Code field. The System displays the Description and any existing Comments for the Contact Title.
2. Click the Insert Record icon on the toolbar. The System creates a blank line under the Code and Description fields to add a new Contact Title.
3. In the Code field, enter the code for the new Contact Title. If the code you choose is already in use for another Contact Title, the System displays a popup box indicating: "Row exists already with same Code." Click on the OK button, delete the Code previously inserted, and

enter another one.
4. TAB to the Description field and enter a description of the new Contact Title.
5. TAB to the Comment field and enter any applicable comments.
6. Click the Save icon.
7. The system displays a pop-up message indicating: "Transaction Completed."
8. Click the OK button.

Update a Contact Title

1. Press the F7 key or click the Query icon.
2. The System automatically clears all of the fields.
3. The cursor moves to the first blank under the Code fields.
4. In the appropriate field, enter either the Code or the Description of the Contact Title being updated.
5. Press the F8 key or the Query icon to execute the query.
6. The System displays any known data corresponding to this Contact Title.
7. Verify that the information displayed is for the Contact Method being updated.
8. Update the Description or Comment as needed. (*Note: The system does not allow updates to the Code itself. If attempted, the system indicates: "Field is protected against update."*)
9. Click the Save icon. The system displays a popup message indicating: "Transaction Completed."
10. Click the OK button.

Delete a Contact Title

1. Press the F7 key or click the Query icon.
2. The System automatically clears all of the fields.
3. The cursor moves to the first blank under the Code fields.
4. In the appropriate field, enter either the Code or the Description of the Contact Title being deleted.
5. Press the F8 key or the Query icon to execute the query.
6. The System displays any known data corresponding to this Contact Title.
7. Verify that the information displayed is for the Contact Title being deleted.
8. Click the Remove Record icon. The system deletes the record from the screen, leaving the fields blank.
9. Click the Save icon. The system displays a popup message indicating: "Transaction Completed."
10. Click the OK button.
11. To verify that the deletion has worked successfully, repeat steps 1-5 above. If the deletion was successful, after pressing the F8 key, the system displays the following error message in a popup message: "Query caused no records to be retrieved. Re-enter."

Figure 16 - Maintain Contact Titles

Fields

Code - This is the user-entered alpha code for the Contact Title. This field is mandatory.
Description - This field is the description for the Contact Title. This field is mandatory.
Comment - The user may provide any comments or remarks. This field is optional.

Maintaining Locales

To Maintain Locales:

1. Click Tables on the System Administration main menu.
2. Click Locales as shown below:
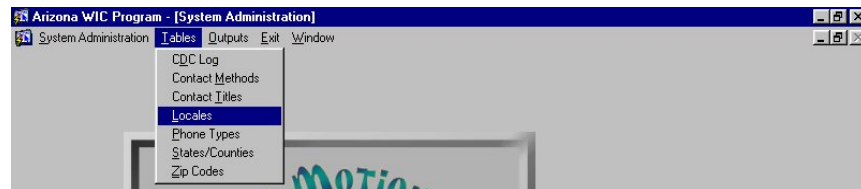
The Maintain Locales window is displayed:
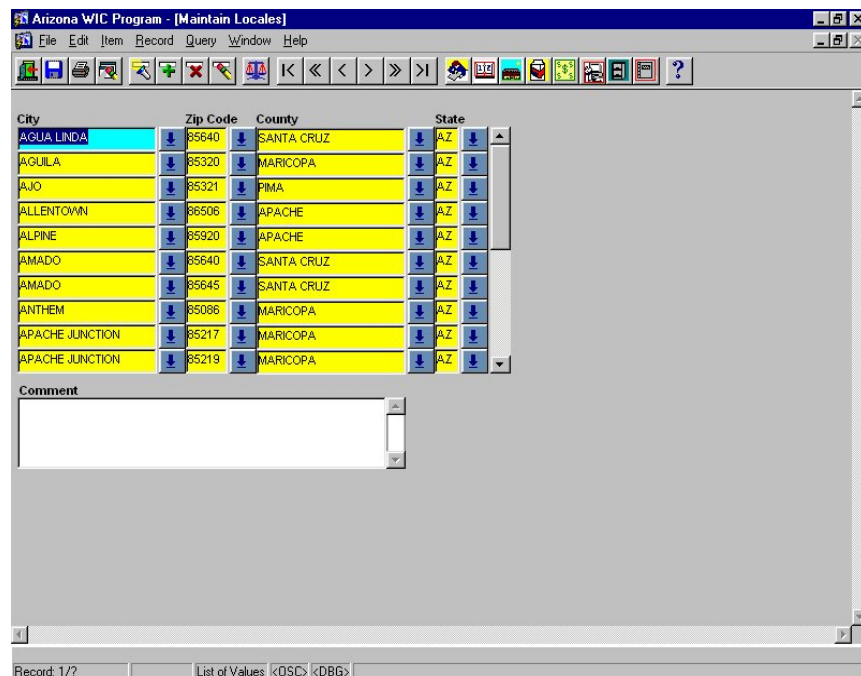
**Figure 17 - Maintain Locales**

Add a Locale

1. The system defaults the cursor to highlight the city under the first entry in the City field. The System displays the Zip Code, County, State, and any existing Comments for the Locale.
2. Click the Insert Record icon on the toolbar. The System creates a blank line under the City, Zip Code, County, and State fields to add a new Locale.
3. Click the list of values button to the right of the blank space under the City field. Select the City for the new locale from the list of values.
4. TAB to the Zip Code field and select the zip code for the new locale from the list of values.
5. TAB to the County field and select the county for the new locale from the list of values.
6. TAB to the State field and select the state for the new locale from the list of values.

7. TAB to the Comment field and enter any applicable comments.
8. Click the Save icon.
9. The system displays a pop-up message indicating: "Transaction Completed."
10. Click the OK button.

Update a Locale

1. Press the F7 key or click the Query icon.
2. The System automatically clears all of the fields.
3. The cursor moves to the first blank under the City fields.
4. In the appropriate field, enter the City being updated.
5. Press the F8 key or the Query icon to execute the query.
6. The System displays any known data corresponding to this Locale.
7. Verify that the information displayed is for the Locale being updated.
8. Update the fields as needed.
9. Click the Save icon. The system displays a popup message indicating: "Transaction Completed."
10. Click the OK button.

Delete a Locale

1. Press the F7 key or click the Query icon.
2. The System automatically clears all of the fields.
3. The cursor moves to the first blank under the City fields.
4. In the appropriate field, enter the City for the Locale being deleted.
5. Press the F8 key or the Query icon to execute the query.
6. The System displays any known data corresponding to this Locale.
7. Verify that the information displayed is for the Locale being deleted.
8. Click the Remove Record icon.
9. Click the Save icon. The system displays a popup message indicating: "Transaction Completed."
10. Click the OK button.
11. To verify that the deletion has worked successfully, repeat steps 1-5 above. If the deletion was successful, after pressing the F8 key, the system displays the following message in a popup window: "Query caused no records to be retrieved. Re-enter."

Figure 17 - Maintain Locales

Fields

City - The user selects the name of the city, which is used to define the geographic location, from the list of values. This field is mandatory.
Zip Code - The user selects the five-digit zip code, which is associated with the geographic location, from the list of values. This field is mandatory.
County - The user selects the name of the county, which is associated with the geographic location, from the list of values. This field is mandatory.
State - The user selects the state abbreviation, which is associated with the geographic location, from the list of values. This field is mandatory.
Comment - Free form text field for the user to enter any information concerning the specified geographic location. This field is optional.

Maintaining Phone Types

To Maintain Phones Types:

1. Click Tables on the System Administration main menu.
2. Click Phones Types as shown below:

The Maintain Phone Types window is displayed:
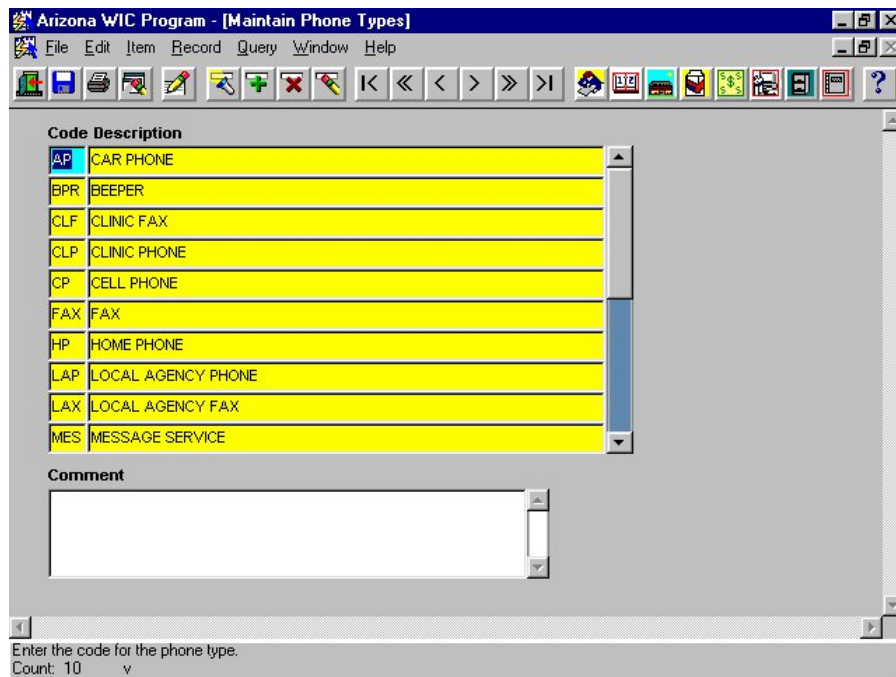
Figure 18 – Maintain Phone Types

Add a Phone Type

1. The system defaults the cursor to highlight the code under the first entry in the Code field. The System displays the Description and any existing Comments for the Phone Type.
2. Click the Insert Record icon on the toolbar. The System creates a blank line under the Code and Description fields to add a new Phone Type.
3. In the Code field, enter the code for the new Phone Type. If the code you choose is already in use for another Phone Type, the System displays a popup window indicating: "Row exists already with same Code." Click on the OK button, delete the Code previously inserted, and enter another one.
4. TAB to the Description field and enter a description of the new Phone Type.

5. TAB to the Comment field and enter any applicable comments.
6. Click the Save icon.
7. The system displays a pop-up message indicating: "Transaction Completed."
8. Click the OK button.

Update a Phone Type

1. Press the F7 key or click the Query icon.
2. The System automatically clears all of the fields.
3. The cursor moves to the first blank under the Code fields.
4. In the appropriate field, enter either the Code or the Description of the Phone Type being updated.
5. Press the F8 key or the Query icon to execute the query.
6. The System displays any known data corresponding to this Phone Type.
7. Verify that the information displayed is for the Phone Type being updated.
8. Update the Description or Comment as needed. (*Note: The system does not allow updates to the Code itself. If attempted, the system indicates: "Field is protected against update."*)
9. Click the Save icon. The system displays a popup message indicating: "Transaction Completed."
10. Click the OK button.

Delete a Phone Type

1. Press the F7 key or click the Query icon.
2. The System automatically clears all of the fields.
3. The cursor moves to the first blank under the Code fields.
4. In the appropriate field, enter either the Code or the Description of the Phone Type being deleted.
5. Press the F8 key or the Query icon to execute the query.
6. The System displays any known data corresponding to this Phone Type.
7. Verify that the information displayed is for the Phone Type being deleted.
8. Click the Remove Record icon. The system deletes the record from the screen, leaving the fields blank.
9. Click the Save icon. The system displays a popup message indicating: "Transaction Completed."
10. Click the OK button.
11. To verify that the deletion has worked successfully, repeat steps 1-5 above. If the deletion was successful, after pressing the F8 key, the system displays the following error message in a popup message: "Query caused no records to be retrieved. Re-enter."

Figure 18 – Maintain Phone Types

Fields

Code - The user assigned code which references a particular form of telecommunication. This field is mandatory.
Description - The explanation of the phone type as it refers to the associated code. This field is mandatory.
Comment - Any free form text that the user may want to enter concerning a particular phone

type. This field is optional.

Maintaining States/Counties

To Maintain States/Counties:

1. Click Tables on the System Administration main menu.
2. Click States/Counties as shown below:
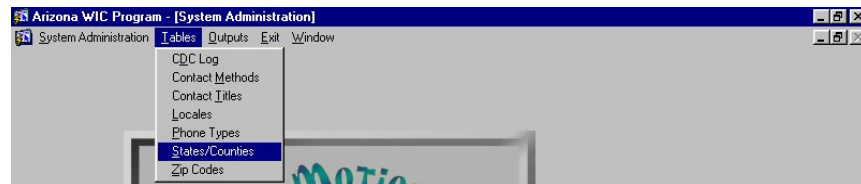
The Maintain States/Countries window is displayed:

Figure 19 - Maintain States/Counties

Add a State/County

1. The system defaults the cursor to highlight the state ID under the first entry in the ID field. The System also displays the Description and any existing Comments for that State.
2. To add a new state, click the Insert Record icon keeping the cursor in the ID field. The System creates a blank line.
3. Enter the abbreviation of the new state in the ID field. If the ID already exists in the system, an error message "The state already exists" is displayed by the System.
4. TAB to the Description field and enter the State name.
5. TAB to the Comments field and enter any comments.
6. TAB to the Code field under the County section, and enter the number for the new county.
7. TAB to the Description field, and enter the name of the new county.

8. TAB to the CDC County Code field, and enter the new code number.
9. TAB to the Comments field under the County section and enter any comments.
10. Click the Save icon.
11. The system displays a pop-up window indicating: "Transaction Completed."
12. Click OK.
13. If the user wants to add a new county to an existing state, query the desired state, click in the code field under the county section, and click the Insert Record icon. The system creates a blank record in the county section. Follow steps 6-10 to enter a new county.

Update a State/County

1. Press the F7 key or click the Query icon.
2. The System automatically clears all of the fields.
3. The cursor moves to the first blank under the State field.
4. In the appropriate field, enter either the State or the Description of the State being updated.
5. Press the F8 key or the Query icon to execute the query.
6. The System displays any known data corresponding to this State.
7. Verify that the information displayed is for the State being updated.
8. Click the Description field under the County section and update any information to be updated. (*Note: The system does not allow updates to the Code or CDC County Code fields. If attempted to do so, the system indicates: "Field is protected against update."*)
9. Click the Save icon. The system displays a popup message indicating: "Transaction Completed."
10. Click the OK button.

Delete a State/County

1. Press the F7 key or click the Query icon.
2. The System automatically clears all of the fields.
3. The cursor moves to the first blank under the State fields.
4. In the appropriate field, enter either the State or the Description of the State/County being deleted.
5. Press the F8 key or the Query icon to execute the query.
6. The System displays any known data corresponding to this State.
7. Verify that the information displayed is for the State or County being deleted.
8. Click the Description field under the State or County section, depending on which section of information to be deleted. When the appropriate Description field is highlighted, click the Remove Record icon.
9. The system deletes the record from the screen, leaving the fields blank.
10. Click the Save icon. The system displays a popup message indicating: "Transaction Completed."
11. Click the OK button.
12. To verify that the deletion has worked successfully, repeat steps 1-5 above. If the deletion was successful, after pressing the F8 key, the system displays the following error message in a popup message: "Query caused no records to be retrieved. Re-enter."

Figure 19 - Maintain States/Counties

Fields

ID - The two letter abbreviation of the state for which the user queries for state/counties. This field is mandatory.

Description - The name of the state for which the user queries for counties. This field is mandatory.

Comment - Free form text field for the user to enter any information concerning the specified state. This field is optional.

Code - The user-entered alphanumeric ID associated with a particular county. This field is mandatory.

Description - The name of the county associated with the code. This field is mandatory.

CDC County Code - The numeric ID of the county assigned by the Center for Disease Control. This field is mandatory.

Comment - Free form text field for the user to enter any information concerning the specified county. This field is optional.

Maintaining Zip Codes

To Maintain Zip Codes:

1. Click Tables on the System Administration main menu.
2. Click Zip Codes as shown below:

The Maintain Zip Codes window is displayed:
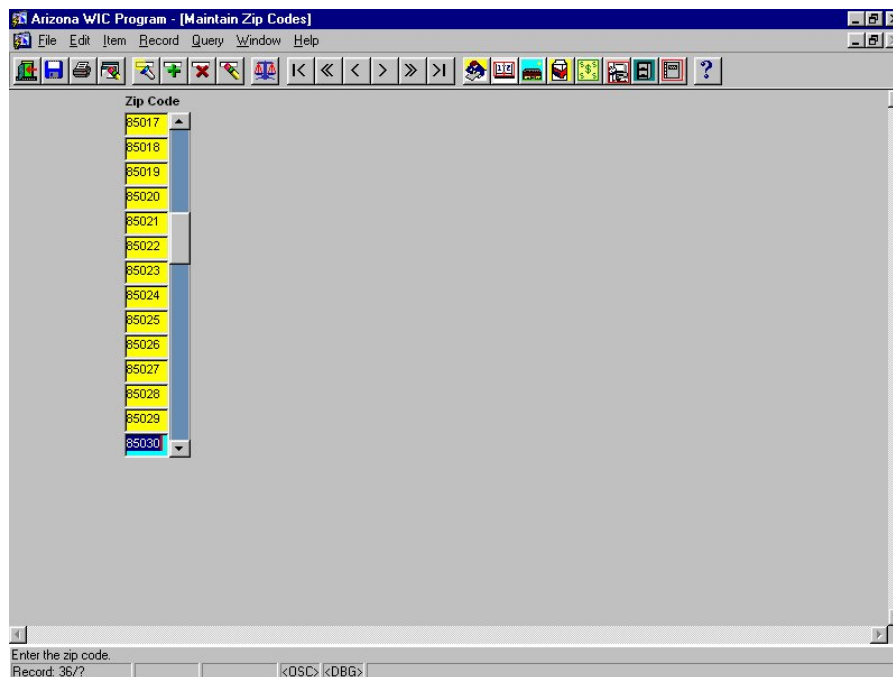
Figure 20 - Maintain Zip Codes

Add a Zip Code

1. The system defaults the cursor to highlight the zip code under the first entry in the Zip Code field.
2. Click the Insert Record icon and the System creates a blank line under the Zip Code field for a new zip code to be added.
3. Enter the new Zip Code number.
4. Click the Save icon.
5. The System displays a pop-up box indicating: "Transaction Completed."
6. Click on the OK button.

Delete a Zip Code

1. Press the F7 key or click the Query icon.
2. The System automatically clears all of the fields.
3. The cursor moves to the first blank under the Zip Code fields.
4. In the appropriate field, enter the Zip Code being deleted.
5. Press the F8 key or the Query icon to execute the query.
6. The System displays the Zip Code.
7. Verify that the information displayed is for the Zip Code being deleted.
8. Click the Remove Record icon.
9. The system deletes the record from the screen, leaving the fields blank.
10. Click the Save icon. The system displays a popup message indicating: "Transaction Completed."
11. Click the OK button.
12. To verify that the deletion has worked successfully, repeat steps 1-5 above. If the deletion was successful, after pressing the F8 key, the system displays the following error message in a popup message: "Query caused no records to be retrieved. Re-enter."

Figure 20 - Maintain Zip Codes

Fields

Zip Code - The list of five digit zip codes. This field is mandatory.

Producing an Expired Passwords Report

To Produce an Expired Passwords Report:

1. Click Outputs on the System Administration main menu
2. Click Expired Passwords as shown below:
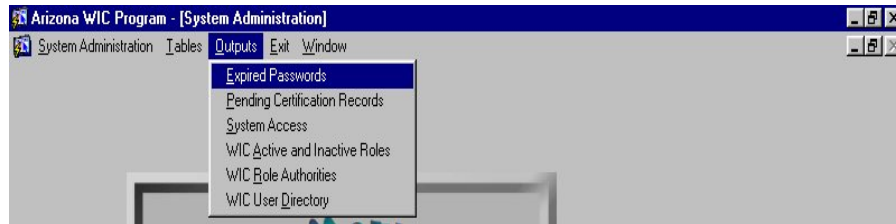
The Expired Passwords parameter window is displayed:
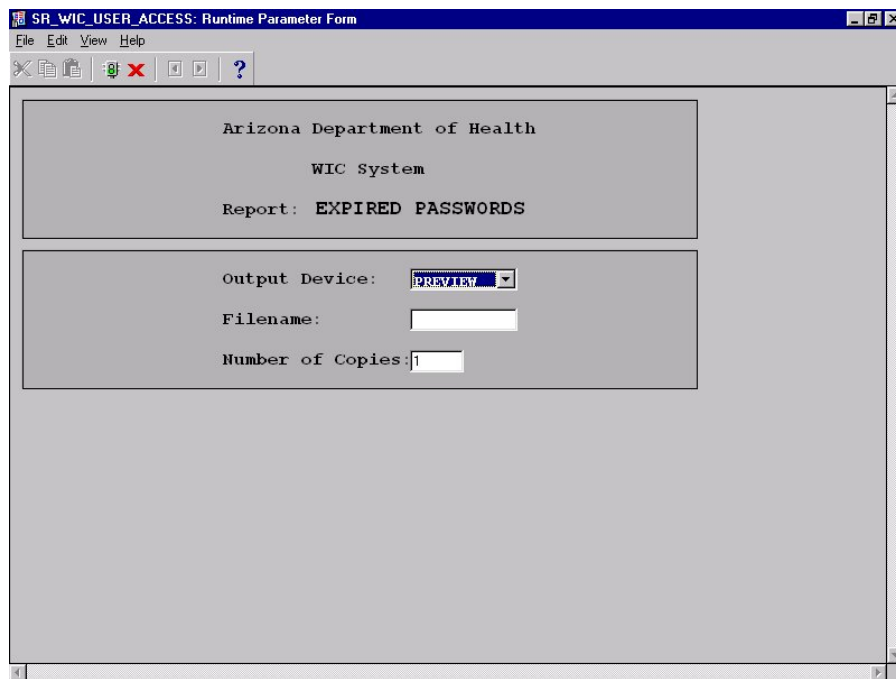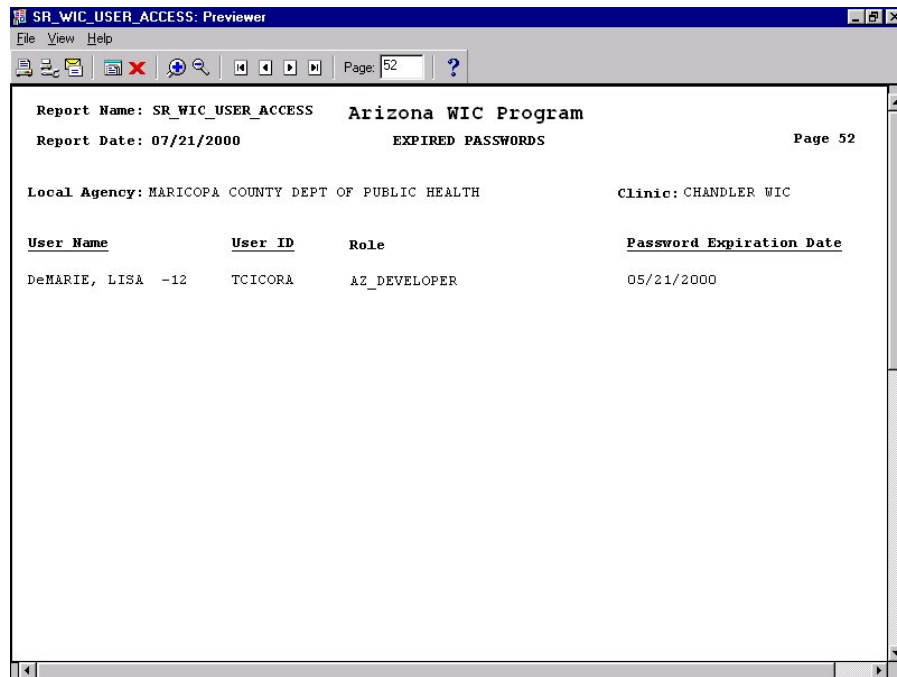
Figure 21 - Expired Passwords Report

Produce an Expired Passwords Report

1. Click the down arrow in the Output Device field to activate the drop down box. Then select which output device the Expired Passwords report should be sent by clicking once on that device name.
2. TAB to the Filename field. If the report is to be saved as a file, enter the filename of the report.
3. TAB to the Number of Copies field. Select the number of report copies desired by typing that number in this field.
4. If Display is selected as the output device, click the green light icon to bring up the preview

report shown below. Otherwise the report is processed per the output device selected.

5. If, at any time, the user decides not to continue, click the Cancel button at the top of the parameter window.

Sample Expired Passwords Report

6. Click the Previous, Next, First, Last, and Page icons at the top of the window to move forward and backward through the report pages.
7. Click the Print icon to print the report.
8. Click the Close icon to exit the preview window.
9. Click the New icon to view a new copy of the same preview window.

Figure 21 - Expired Passwords Report

Fields

Output Device - The user may select (from a drop down list) display (window), file, or printer.
Filename - If file is selected (above), the directory and filename are entered.
Number of Copies - If printer is selected (above), the number of copies desired is entered.

Producing a Pending Certifications Record Report

To Produce a Pending Certifications Record Report:

1. Click Outputs on the System Administration main menu.
2. Click Pending Certification Records as shown below:

The Pending Certifications Records parameter window is displayed:
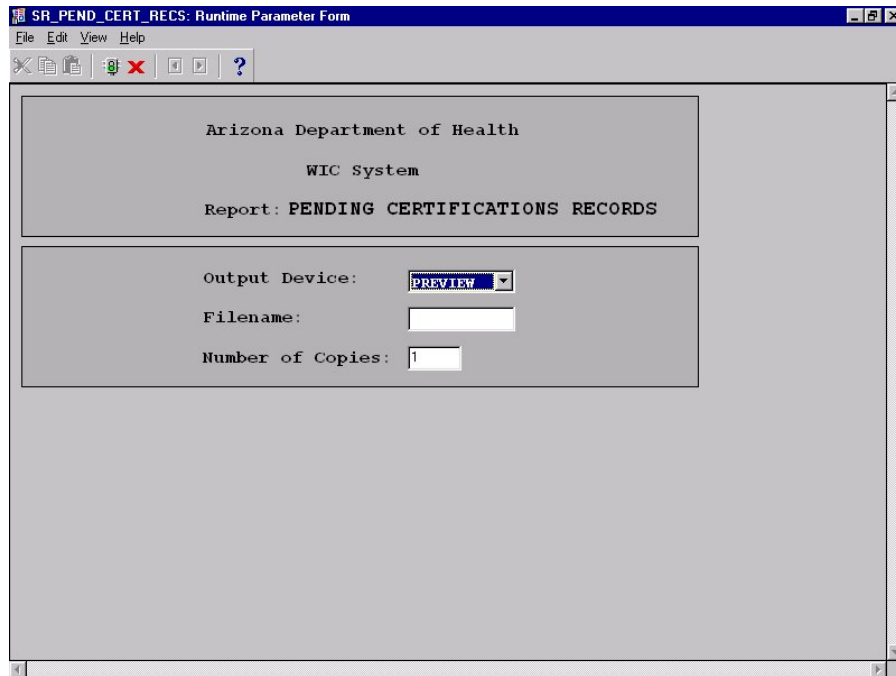
Figure 22 - Pending Certifications Records Report

Produce Pending Certifications Records Report

1. Click the down arrow in the Output Device field to activate the drop down box. Then select which output device the Pending Certifications Records report should be sent by clicking once on that device name.
2. TAB to the Filename field. If the report is to be saved as a file, enter the filename of the report.
3. TAB to the Number of Copies field. Select the number of report copies desired by typing that number in this field.
4. If Display is selected as the output device, click the green light icon to bring up the preview report shown below. Otherwise the report is processed per the output device selected.
5. If, at any time, the user decides not to continue, click the Cancel button at the top of the parameter window.

Sample Pending Certifications Records Report

6. Click the Previous, Next, First, Last, and Page icons at the top of the window to move forward and backward through the report pages.
7. Click the Print icon to print the report.
8. Click the Close icon to exit the preview window.
9. Click the New icon to view a new copy of the same preview window.

Figure 22 - Pending Certifications Records Report

Fields

Output Device - The user may select (from a drop down list) display (window), file or printer.
Filename - If file is selected (above), the directory and filename are entered.
Number of Copies - If printer is selected (above), the number of copies desired is entered.
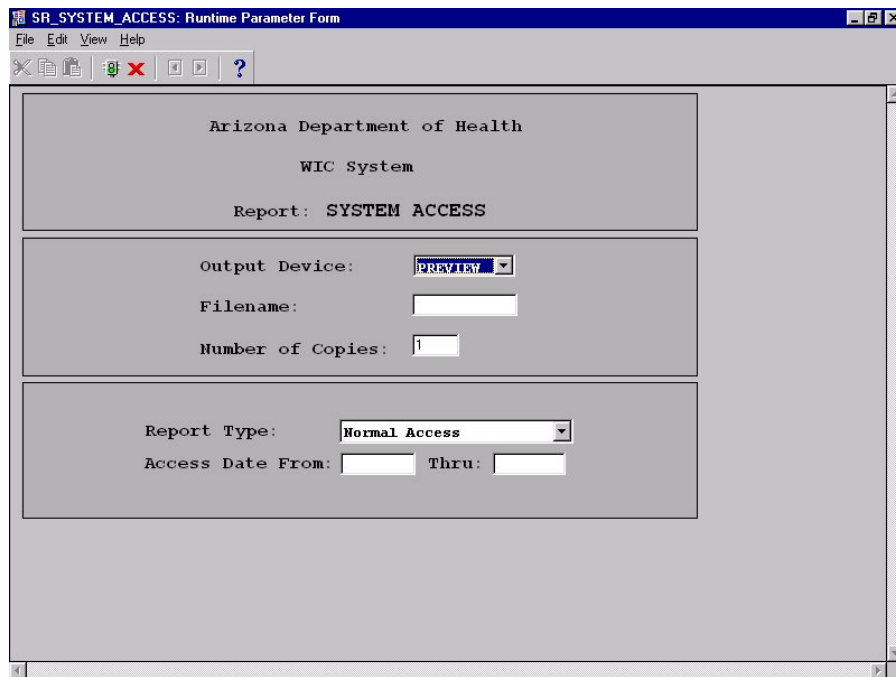
Producing a System Access Report

To Produce a System Access Report:

1. Click Outputs on the System Administration main menu.
2. Click System Access as shown below:
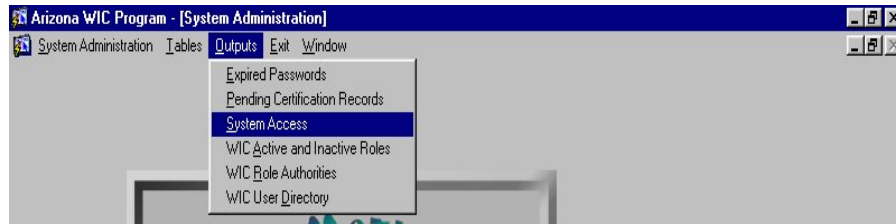
The System Access parameter window is displayed:

Figure 23 – System Access Report

Produce a System Access Report

1. Click the down arrow in the Output Device field to activate the drop down box. Then select which output device the System Access report should be sent by clicking once on that device name.
2. TAB to the Filename field. If the report is to be saved as a file, enter the filename of the report.
3. TAB to the Number of Copies field. Select the number of report copies desired by typing that number in this field.

4. TAB to the Report Type and select the desired report type (Normal, Unusual, Unauthorized, etc.) from the drop-down list.
5. TAB to the Access Date From field and enter the beginning access date to be covered. This date must be formatted MM/DD/YYYY.
6. TAB to the Thru field and enter the ending access date to be covered using the format MM/DD/YYYY.
7. If Display is selected as the output device, click the green light icon to bring up the preview report shown below. Otherwise the report is processed per the output device selected.
8. If, at any time, the user decides not to continue, click the Cancel button at the top of the parameter window.

Sample System Access Report

9. Click the Previous, Next, First, Last, and Page icons at the top of the window to move forward and backward through the report pages.
10. Click the Print icon to print the report.
11. Click the Close icon to exit the preview window.
12. Click the New icon to view a new copy of the same preview window.

Figure 23 – System Access Report

Fields

Output Device - The user may select (from a drop down list) display (window), file or printer.
**Filename** - If file is selected (above), the directory and filename are entered.
Number of Copies - If printer is selected (above), the number of copies desired is entered.
Report Type - The user selects the desired report type (Normal, Unusual, Unauthorized, etc.) from the drop-down list.

Access Date From/Thru - The range of dates upon which the report filters data, excluding information not falling within the specified range. These fields are mandatory.

Producing a WIC Active and Inactive Roles Report

To Produce a WIC Active and Inactive Roles Report:

1. Click Outputs on the System Administration main menu.
2. Click WIC Active and Inactive Roles as shown below:
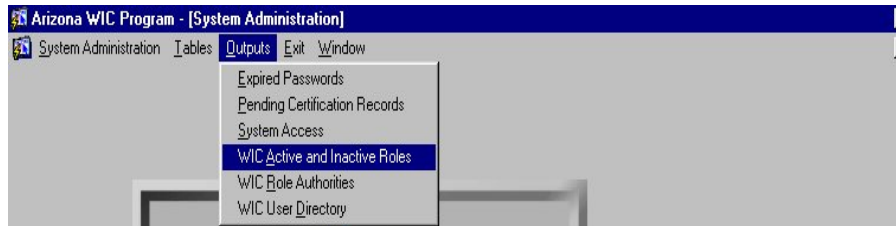
The WIC Active and Inactive Roles parameter window is displayed:
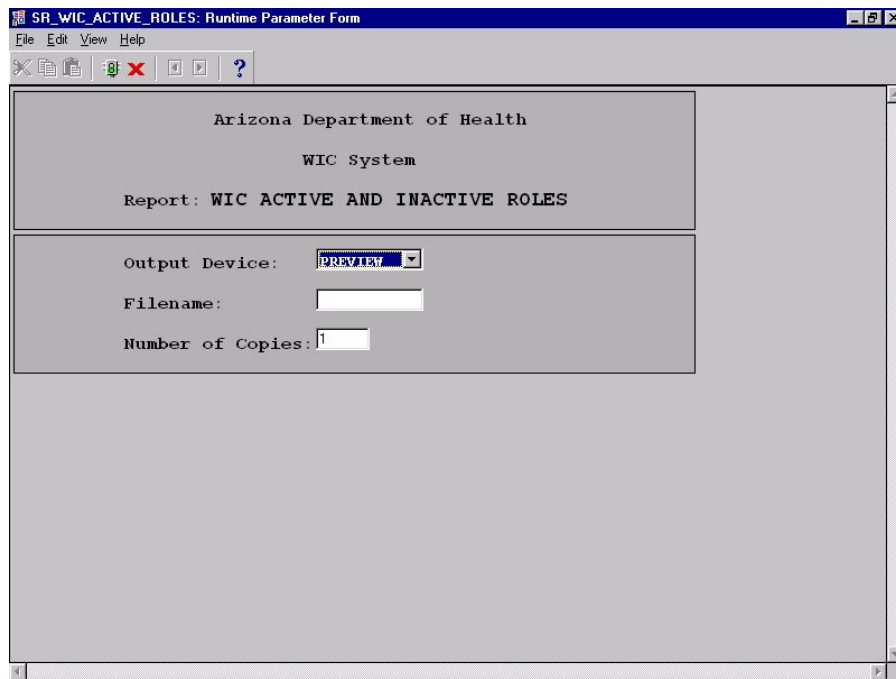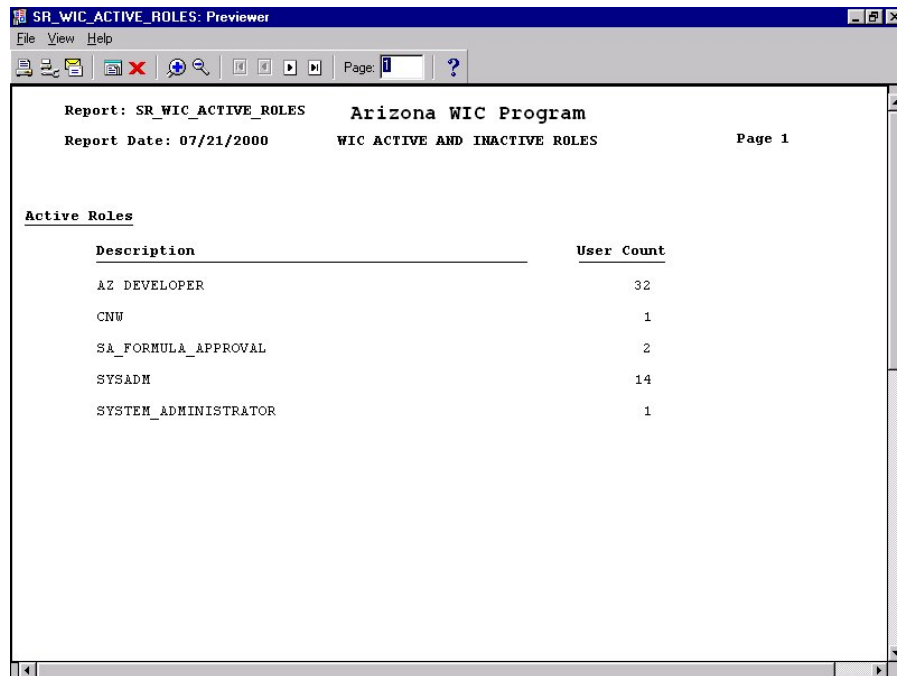
Figure 24 - WIC Active and Inactive Roles

Produce a WIC Active and Inactive Roles Report

1. Click the down arrow in the Output Device field to activate the drop down box. Then select which output device the WIC Active and Inactive Roles report should be sent by clicking once on that device name.
2. TAB to the Filename field. If the report is to be saved as a file, enter the filename of the report.
3. TAB to the Number of Copies field. Select the number of report copies desired by typing that number in this field.

4. If Display is selected as the output device, click the green light icon to bring up the preview report shown below. Otherwise the report is processed per the output device selected.
5. If, at any time, the user decides not to continue, click the Cancel button at the top of the parameter window.

Sample WIC Active and Inactive Roles Report

6. Click the Previous, Next, First, Last, and Page icons at the top of the window to move forward and backward through the report pages.
7. Click the Print icon to print the report.
8. Click the Close icon to exit the preview window.
9. Click the New icon to view a new copy of the same preview window.

Figure 24 - WIC Active and Inactive Roles

Fields

Output Device - The user may select (from a drop down list) display (window), file, or printer.
Filename - If file is selected (above), the directory and filename are entered.
Number of Copies - If printer is selected (above), the number of copies desired is entered.
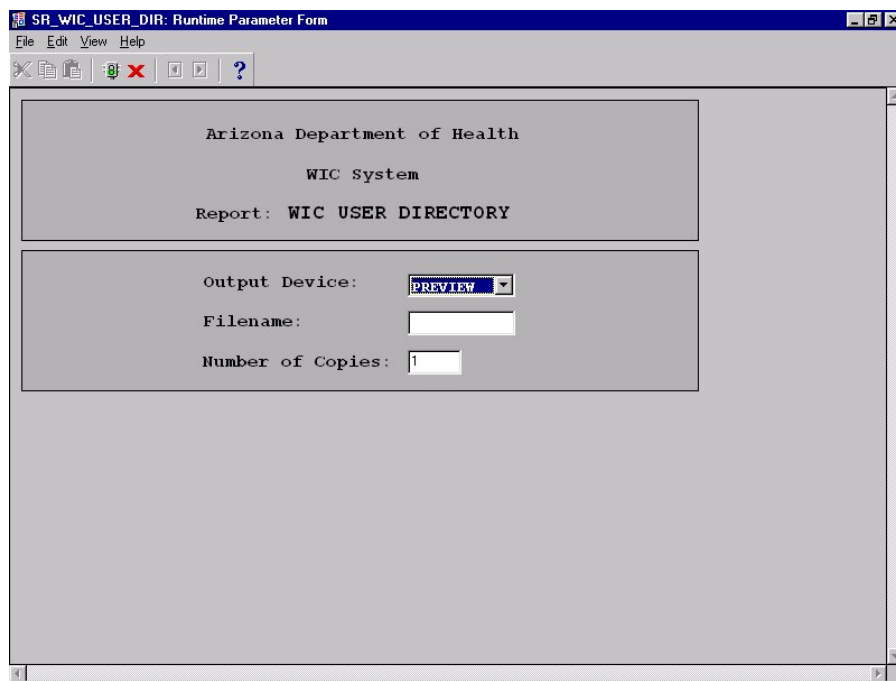
Producing a WIC Role Authorities Report

To Produce a WIC Role Authorities Report:

1. Click Outputs on the System Administration main menu.
2. Click WIC Role Authorities as shown below:
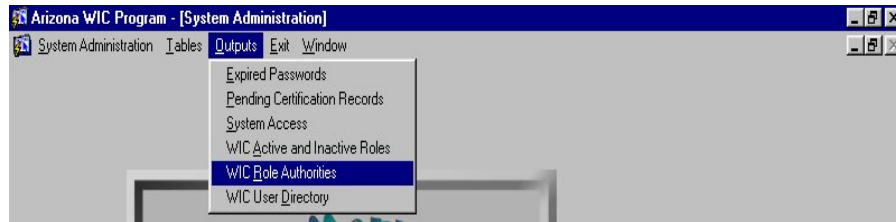
The WIC Role Authorities parameter window is displayed:
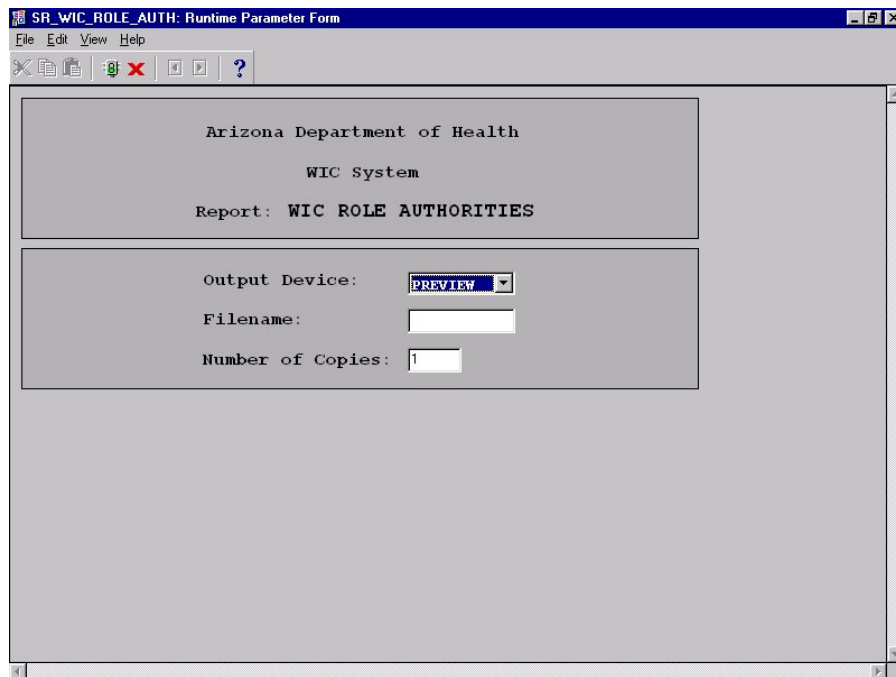
Figure 25 - WIC Role Authorities

Produce a WIC Role Authorities Report

1. Click the down arrow in the Output Device field to activate the drop down box. Then select which output device the WIC Role Authorities report should be sent by clicking once on that device name.
2. TAB to the Filename field. If the report is to be saved as a file, enter the filename of the report.
3. TAB to the Number of Copies field. Select the number of report copies desired by typing that number in this field.
4. If Display is selected as the output device, click the green light icon to bring up the preview report shown below. Otherwise the report is processed per the output device selected.

5. If, at any time, the user decides not to continue, click the Cancel button at the top of the parameter window.

Sample WIC Role Authorities Report

6. Click the Previous, Next, First, Last, and Page icons at the top of the window to move forward and backward through the report pages.
7. Click the Print icon to print the report.
8. Click the Close icon to exit the preview window.
9. Click the New icon to view a new copy of the same preview window.

Figure 25 - WIC Role Authorities

Fields

Output Device - The user may select (from a drop down list) display (window), file or printer.
Filename - If file is selected (above), the directory and filename are entered.
Number of Copies - If printer is selected (above), the number of copies desired is entered.

Producing a WIC User Directory Report

To Produce a WIC User Directory Report:

1. Click Outputs on the System Administration main menu.
2. Click WIC User Directory as shown below:

The WIC User Directory parameter window is displayed:
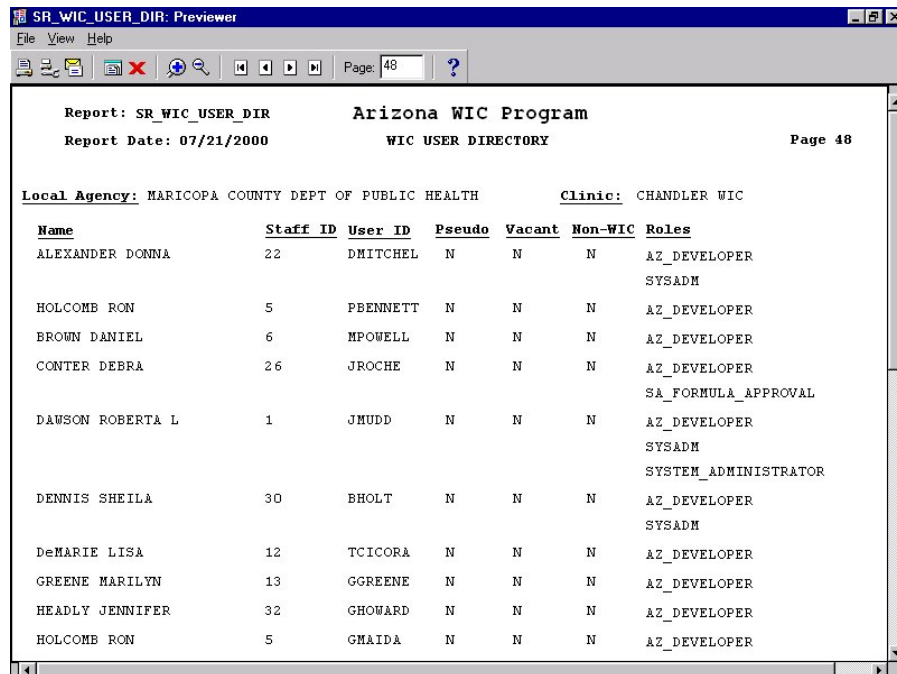
Figure 26 - WIC User Directory Report

Produce a WIC User Directory Report

1. Click the down arrow in the Output Device field to activate the drop down box. Then select
   to which output device the WIC User Directory report should be sent by clicking once on that
   device name.
2. TAB to the Filename field. If the report is to be saved as a file, enter the filename of the
   report.
3. TAB to the Number of Copies field. Select the number of report copies desired by typing
   that number in this field.

4. If Display is selected as the output device, click the green light icon to bring up the preview report shown below. Otherwise the report is processed per the output device selected.
5. If, at any time, the user decides not to continue, click the Cancel button at the top of the parameter window.

Sample WIC User Directory Report

6. Click the Previous, Next, First, Last, and Page icons at the top of the window to move forward and backward through the report pages.
7. Click the Print icon to print the report.
8. Click the Close icon to exit the preview window.
9. Click the New icon to view a new copy of the same preview window.

Figure 26 - WIC User Directory Report

Fields

Output Device - The user may select (from a drop down list) display (window), file, or printer.
Filename - If file is selected (above), the directory and filename are entered.
Number of Copies - If printer is selected (above), the number of copies desired is entered.

List of Figures